McAfee® Wireless Protection 2007

Guida dell'utente

Sommario

CAPITOLO 1

McAfee Wireless Protection

McAfee Wireless Protection Suite elimina i problemi di rete e i rischi per la protezione delle reti senza fili e fornisce una protezione affidabile che consente di impedire agli hacker di attaccare la rete Wi-Fi®, proteggere i dati e le transazioni personali e bloccare l'utilizzo non autorizzato della rete per accedere a Internet, il tutto con un semplice clic del mouse. In McAfee Wireless Network Security, la rotazione automatica di complesse chiavi di crittografia si dimostra efficace anche contro gli intrusi più determinati. Wireless Protection include anche McAfee EasyNetwork che semplifica la condivisione di file e stampanti in rete. Inoltre, viene fornito con McAfee Network Manager, che monitora i computer in rete alla ricerca di eventuali vulnerabilità nella protezione e semplifica la soluzione dei potenziali problemi di protezione.

In Wireless Protection sono inclusi i seguenti programmi:

- SecurityCenter
- Wireless Network Security
- Network Manager
- EasyNetwork

CAPITOLO 2

McAfee SecurityCenter

McAfee SecurityCenter è un ambiente di facile utilizzo, che consente agli utenti McAfee di avviare, gestire e configurare i propri abbonamenti ai prodotti di protezione.

SecurityCenter fornisce inoltre informazioni su avvisi relativi ai virus, prodotti, supporto tecnico e abbonamenti nonché un accesso rapido a strumenti e notizie presenti sul sito Web di McAfee.

In questo capitolo

Funzioni

McAfee SecurityCenter offre le nuove funzioni e i vantaggi riportati di seguito:

Stato di protezione riprogettato

Consente un controllo semplificato dello stato di protezione del computer, la verifica della disponibilità di aggiornamenti e la risoluzione dei potenziali problemi di protezione.

Aggiornamenti continui

L'installazione di aggiornamenti quotidiani avviene automaticamente. Quando una nuova versione di software McAfee è disponibile, verrà scaricata automaticamente senza alcun costo ulteriore nel corso dell'abbonamento, garantendo quindi una protezione sempre aggiornata.

Avvisi in tempo reale

Gli avvisi di protezione notificano all'utente la diffusione di virus e di minacce per la protezione e forniscono opzioni di risposta che consentono di rimuovere e neutralizzare la minaccia o di ottenere ulteriori informazioni su di essa.

Protezione conveniente

Un'ampia gamma di opzioni di rinnovo consente di mantenere aggiornata l'attuale protezione McAfee.

Strumenti per il rendimento

È possibile rimuovere i file inutilizzati, deframmentare quelli utilizzati e servirsi del ripristino della configurazione di sistema per ottenere sempre prestazioni ottimali dal proprio computer.

Guida in linea in tempo reale

Consente di ricevere assistenza tramite chat Internet, posta elettronica e telefono dagli esperti di protezione dei computer di McAfee.

Navigazione protetta e sicura

Se installato, il plug-in per browser McAfee SiteAdvisor consente di proteggere il computer da spyware, posta indesiderata, virus e frodi in linea tramite un sistema di classificazione dei siti Web visitati o riportati nei risultati delle ricerche effettuate sul Web. È possibile visualizzare una classificazione di sicurezza che indica in dettaglio la valutazione di un sito in relazione a gestione della posta elettronica, esecuzione dei download, iscrizioni online e disturbi quali popup e cookie traccianti di terze parti.

CAPITOLO 3

Utilizzo di SecurityCenter

È possibile avviare SecurityCenter dall'icona di McAfee SecurityCenter , situata nell'area di notifica di Windows all'estremità destra della barra delle applicazioni, oppure dal desktop di Windows.

Quando si apre SecurityCenter, il riquadro Home visualizza lo stato di protezione del computer e consente di accedere rapidamente alle funzioni di aggiornamento, alle scansioni (se è stato installato McAfee VirusScan) e ad altre attività comuni.

Intestazione

Guida in linea

Visualizza il file della guida in linea del programma.

Colonna di sinistra

Aggiorna

Aggiorna il prodotto per assicurare la protezione dalle minacce più recenti.

Scansione

Se è stato installato McAfee VirusScan, è possibile eseguire una scansione manuale del computer.

Attività comuni

Consente di eseguire le attività comuni, tra cui il ritorno al riquadro Home, la visualizzazione degli eventi più recenti, la gestione della rete di computer (nel caso in cui si tratti di un computer con capacità di gestione della rete), nonché la manutenzione del computer. Se è stato installato McAfee Data Backup, è anche possibile eseguire il backup dei dati.

Componenti installati

Consente di visualizzare i servizi di protezione attivi sul computer in uso.

Riquadro principale

Stato protezione

La sezione **Il computer è protetto?** indica il livello di protezione generale del computer. Nella sezione sottostante sono visualizzati i dettagli dello stato suddivisi per tipo e per categoria di protezione.

Informazioni su SecurityCenter

Consente di visualizzare la data dell'ultimo aggiornamento del computer, la data dell'ultima scansione (se è stato installato McAfee VirusScan) e la data di scadenza dell'abbonamento.

In questo capitolo

Informazioni sulle icone di SecurityCenter

Le icone di SecurityCenter vengono visualizzate nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni. È possibile utilizzarle per verificare se il computer è protetto, consultare lo stato di una scansione in corso (se è stato installato McAfee VirusScan), controllare la disponibilità di aggiornamenti, visualizzare gli eventi recenti, eseguire la manutenzione del computer e ottenere assistenza dal sito web di McAfee.

Apertura di SecurityCenter e utilizzo delle funzioni aggiuntive

Quando SecurityCenter è in esecuzione, l'icona M viene visualizzata nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni.

Per aprire SecurityCenter o utilizzare le funzioni aggiuntive

- Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, quindi selezionare uno dei seguenti comandi:
  - Apri SecurityCenter
  - Aggiornamenti
  - Collegamenti rapidi

    Il sottomenu contiene collegamenti a Home, Visualizza eventi recenti, Gestione rete, Manutenzione computer e Data Backup (se installato).
  - Verifica abbonamento

    Questa voce viene visualizzata quando l'abbonamento di almeno un prodotto è scaduto.
  - Centro aggiornamenti
  - Servizio clienti

Verifica dello stato di protezione

Se il computer non è completamente protetto, l'icona dello stato di protezione viene visualizzata nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni. L'icona può essere rossa o gialla in base allo stato di protezione.

Per verificare dello stato di protezione

- Fare clic sull'icona dello stato di protezione per aprire SecurityCenter e risolvere eventuali problemi.

Verifica dello stato degli aggiornamenti

Se è in corso la verifica della disponibilità degli aggiornamenti, l'icona degli aggiornamenti viene visualizzata nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni.

Per verificare lo stato degli aggiornamenti

- Scegliere l'icona degli aggiornamenti per visualizzare una breve descrizione dello stato degli aggiornamenti.

Informazioni sullo stato della protezione

Lo stato di protezione generale del computer viene visualizzato nella sezione **Il computer è protetto?** di SecurityCenter.

Lo stato della protezione indica se il computer è protetto nei confronti delle più recenti minacce alla sicurezza, se permangono problemi che richiedono attenzione e il modo in cui affrontarli. Quando un problema interessa più di una categoria di protezione, la sua risoluzione può avere come effetto il ritorno allo stato di protezione completa di più categorie.

Lo stato della protezione è influenzato da alcuni fattori, tra cui le minacce esterne, i prodotti di protezione o di accesso a Internet installati nel computer e la configurazione di tali prodotti.

Per impostazione predefinita, se non sono installati prodotti di protezione dalla posta indesiderata o di blocco dei contenuti, i problemi di protezione secondari controllati da tali prodotti vengono automaticamente ignorati e non vengono considerati nello stato di protezione generale. Tuttavia, se un problema di protezione è seguito da un collegamento **Ignora** , è possibile scegliere di ignorare il problema se si è certi di non avere la necessità di risolverlo.

Il computer è protetto?

Il livello generale di protezione del computer può essere visualizzato nella sezione **Il computer è protetto?** di SecurityCenter:

- Se il computer è protetto, viene visualizzato **Sì** (in verde).
- Se il computer è parzialmente protetto o non protetto, viene visualizzato **No**, rispettivamente in giallo o in rosso.

Per risolvere automaticamente la maggior parte dei problemi di protezione, fare clic su **Correggi** accanto allo stato di protezione. Tuttavia, se uno o più problemi persistono e richiedono un intervento, fare clic sul collegamento visualizzato accanto al problema per intraprendere le azioni consigliate.

Informazioni sulle categorie e i tipi di protezione

Nella sezione **Il computer è protetto?** di SecurityCenter è possibile visualizzare i dettagli dello stato, costituito dai seguenti tipi e categorie di protezione:

- Computer e file
- Rete e Internet
- Posta elettronica e MI
- Controllo genitori

I tipi di protezione visualizzati da SecurityCenter dipendono dai prodotti installati. Ad esempio, il tipo di protezione Stato del computer viene visualizzato se è stato installato il software McAfee Data Backup.

Se una categoria non presenta alcun problema di protezione, lo stato è Verde. Se si fa clic su una categoria Verde, viene visualizzato a destra un elenco di tipi di protezione attivati, seguito da un elenco di problemi già ignorati. Se non esistono problemi, viene visualizzato un avviso virus. È inoltre possibile fare clic su **Configura** per modificare le opzioni relative a una determinata categoria.

Se lo stato è Verde per tutti i tipi di protezione di una stessa categoria, anche lo stato della categoria sarà Verde. Analogamente, se lo stato di tutte le categorie di protezione è Verde, lo Stato di protezione generale sarà Verde.

Se lo stato di alcune categorie di protezione è Giallo o Rosso, è possibile risolvere i problemi di protezione correggendoli o ignorandoli e in entrambi i casi lo stato diventerà Verde.

Informazioni sulla protezione di computer e file

La categoria di protezione Computer e file comprende i seguenti tipi di protezione:

- **Protezione da virus**: protezione con scansione in tempo reale che difende il computer da virus, worm, trojan horse, script sospetti, attacchi di vario genere e altre minacce. Analizza e automaticamente tenta di pulire i file, compresi file eseguibili compressi, settore di avvio, memoria e file essenziali, quando viene eseguito l'accesso dall'utente o dal computer.
- **Protezione da spyware**: rileva, blocca e rimuove rapidamente programmi spyware, adware e altri programmi potenzialmente indesiderati che potrebbero raccogliere e trasmettere i dati personali senza l'autorizzazione dell'utente.
- **SystemGuards**: moduli che rilevano le modifiche apportate al computer e le segnalano all'utente. È quindi possibile esaminare le modifiche e decidere se consentirle.
- **Protezione di Windows**: la protezione di Windows fornisce lo stato dell'aggiornamento di Windows sul computer. Se è stato installato McAfee VirusScan, è inoltre disponibile la protezione da sovraccarico del buffer.

Uno dei fattori che influenzano la protezione di computer e file è costituito dalle minacce esterne di virus. Ad esempio, in caso di diffusione di un virus, è opportuno verificare se il software antivirus in uso è in grado di proteggere il computer. Altri fattori possono essere la configurazione del software antivirus e la frequenza con cui il software viene aggiornato in base ai nuovi file delle firme per i rilevamenti, in modo da proteggere il computer dalle minacce più recenti.

Apertura del riquadro di configurazione File e computer

Se in **File & computer** non sono stati rilevati problemi, è possibile aprire il riquadro di configurazione dal riquadro di informazioni.

Per aprire il riquadro di configurazione File e computer

1. Nel riquadro Home, fare clic su **File & computer**.
2. Nel riquadro di destra, fare clic su **Configura**.

Informazioni sulla protezione di Internet e rete

La categoria di protezione Rete e Internet comprende i seguenti tipi di protezione:

- **Protezione firewall**: consente di difendere il computer da intrusioni e da traffico di rete indesiderato e agevola la gestione delle connessioni Internet in entrata e in uscita.
- **Wireless Protection**: consente di proteggere la rete wireless domestica da intrusioni e intercettazioni di dati. Tuttavia, se attualmente si è connessi a una rete wireless esterna, il livello di protezione varia a seconda del livello di sicurezza di quella rete.
- **Protezione navigazione Web**: la protezione della navigazione sul Web consente di nascondere pubblicità, popup e Web bug sul computer durante la navigazione su Internet.
- **Protezione da phishing**: consente di bloccare i siti Web fraudolenti che richiedono l'invio di dati personali tramite collegamenti ipertestuali visualizzati in messaggi di posta elettronica, messaggi immediati, popup e in altri elementi.
- **Protezione dei dati personali**: blocca la diffusione dei dati sensibili e riservati su Internet.

Apertura del riquadro di configurazione Internet e rete

Se in **Internet & rete** non sono stati rilevati problemi, è possibile aprire il riquadro di configurazione dal riquadro di informazioni.

Per aprire il riquadro di configurazione Internet e rete

1. Nel riquadro Home, fare clic su **Internet & rete**.
2. Nel riquadro di destra, fare clic su **Configura**.

Informazioni sulla protezione di posta elettronica e MI

La categoria di protezione Posta elettronica e MI comprende i seguenti tipi di protezione:

- **Protezione della posta elettronica**: analizza e automaticamente tenta di eliminare i virus, i programmi spyware e le minacce potenziali presenti nei messaggi e negli allegati di posta elettronica in ingresso e in uscita.
- **Protezione da posta indesiderata**: consente di bloccare l'accesso alla Posta in arrivo dei messaggi di posta elettronica indesiderati.
- **Protezione MI**: la protezione della messaggistica immediata (MI) esamina e automaticamente tenta di eliminare i virus, i programmi spyware e le minacce potenziali presenti negli allegati ai messaggi immediati in ingresso. Impedisce inoltre ai client di messaggistica immediata di scambiare contenuti indesiderati o informazioni personali su Internet.
- **Navigazione protetta e sicura**: se installato, il plug-in per browser McAfee SiteAdvisor consente di proteggere il computer da spyware, spam, virus e frodi in linea tramite un sistema di classificazione dei siti Web visitati o riportati nei risultati delle ricerche effettuate sul Web. È possibile visualizzare una classificazione di sicurezza che indica in dettaglio la valutazione di un sito in relazione a gestione della posta elettronica, esecuzione dei download, iscrizioni online e disturbi quali popup e tracking cookie di terze parti.

Apertura del riquadro di configurazione Posta elettronica e MI

Se in **Posta elettronica & MI** non sono stati rilevati problemi, è possibile aprire il riquadro di configurazione dal riquadro di informazioni.

Per aprire il riquadro di configurazione Posta elettronica e MI

1. Nel riquadro Home, fare clic su **Posta elettronica & MI**.
2. Nel riquadro di destra, fare clic su **Configura**.

Informazioni sulla protezione Controllo genitori

La categoria di protezione Controllo genitori comprende i seguenti tipi di protezione:

- **Controllo genitori**: la funzione di blocco dei contenuti impedisce agli utenti di visualizzare i contenuti Internet indesiderati bloccando i siti Web potenzialmente dannosi. È anche possibile monitorare e limitare l'attività degli utenti di Internet.

Apertura del riquadro di configurazione Controllo genitori

Se in **Controllo genitori** non sono stati rilevati problemi, è possibile aprire il riquadro di configurazione dal riquadro di informazioni.

Per aprire il riquadro di configurazione Controllo genitori

1. Nel riquadro Home, fare clic su **Controllo genitori**.
2. Nel riquadro di destra, fare clic su **Configura**.

Risoluzione dei problemi di protezione

La maggior parte dei problemi di protezione può essere risolta automaticamente. Tuttavia, se uno o più problemi persistono, è necessario risolverli.

Risoluzione automatica dei problemi di protezione

È possibile risolvere automaticamente la maggior parte dei problemi di protezione.

Per risolvere automaticamente i problemi di protezione

- Fare clic su **Correggi** accanto allo stato di protezione.

Risoluzione manuale dei problemi di protezione

Se uno o più problemi non vengono risolti automaticamente, fare clic sul collegamento accanto al problema e intraprendere le azioni consigliate.

Per risolvere manualmente i problemi di protezione

- Effettuare una delle seguenti operazioni:
  - Se non è stata eseguita una scansione completa del computer negli ultimi 30 giorni, fare clic su **Scansione** a sinistra dello stato di protezione principale, per eseguire una scansione manuale. Questa voce viene visualizzata solo se è installato McAfee VirusScan.
  - Se i file delle firme per i rilevamenti (DAT) non sono aggiornati, fare clic su **Aggiorna** a sinistra dello stato di protezione principale per aggiornare la protezione.
  - Se un programma non è installato, fare clic su **Protezione completa** per installarlo.
  - Se in un programma mancano alcuni componenti, sarà necessario reinstallarlo.
  - Nel caso in cui sia necessario registrare un programma per ottenere la protezione completa, fare clic su **Registra adesso** per effettuare la registrazione. Questa voce viene visualizzata se uno o più programmi sono scaduti.
  - Se un programma è scaduto, fare clic su **Verifica abbonamento** per controllare lo stato dell'account. Questa voce viene visualizzata se uno o più programmi sono scaduti.

Visualizzazione delle informazioni su SecurityCenter

Nella parte inferiore del riquadro dello stato della protezione, Informazioni su SecurityCenter consente di accedere alle opzioni di SecurityCenter e di visualizzare i dati relativi all'ultimo aggiornamento, all'ultima scansione eseguita (se è installato McAfee VirusScan) e alla scadenza dell'abbonamento dei prodotti McAfee installati.

Apertura del riquadro di configurazione di SecurityCenter

Per comodità, dal riquadro Home è possibile aprire il riquadro di configurazione di SecurityCenter per modificare le opzioni.

Per aprire il riquadro di configurazione di SecurityCenter

- Nel riquadro Home, in **Informazioni su SecurityCenter**, fare clic su **Configura**.

Visualizzazione delle informazioni sui prodotti installati

È possibile visualizzare un elenco dei prodotti installati che mostri il numero della versione di ogni prodotto e la data dell'ultimo aggiornamento.

Per visualizzare le informazioni sui prodotti McAfee

- Nel riquadro Home, in **Informazioni su SecurityCenter**, fare clic su **Visualizza dettagli** per aprire la finestra di informazioni sul prodotto.

Utilizzo del menu avanzato

Quando si apre per la prima volta SecurityCenter, nella colonna di sinistra viene visualizzato il menu standard. Gli utenti esperti possono accedere a un menu più dettagliato facendo clic su **Menu avanzato**. Per praticità, ogni volta che si apre SecurityCenter viene visualizzato il menu utilizzato la volta precedente.

Il menu avanzato contiene i seguenti elementi:

- Home
- Rapporti e registri (comprende l'elenco Eventi recenti e i registri ordinati per tipo per i 30, 60 e 90 giorni precedenti).
- Configura
- Ripristina
- Strumenti

CAPITOLO 4

Configurazione delle opzioni di SecurityCenter

SecurityCenter visualizza lo stato generale di protezione del computer, consente di creare gli account utente McAfee, installa automaticamente gli aggiornamenti più recenti dei prodotti e segnala automaticamente all'utente, mediante avvisi e segnali acustici, la diffusione di virus, il rilevamento di minacce e la disponibilità di aggiornamenti dei prodotti.

Nel riquadro Configurazione di SecurityCenter, è possibile modificare le opzioni per le seguenti funzioni:

- Stato protezione
- Utenti
- Aggiornamenti automatici
- Avvisi

In questo capitolo

Configurazione dello stato della protezione

Lo stato di protezione generale del computer viene visualizzato nella sezione **Il computer è protetto?** di SecurityCenter.

Lo stato della protezione indica se il computer è protetto nei confronti delle più recenti minacce alla sicurezza, se permangono problemi che richiedono attenzione e il modo in cui affrontarli.

Per impostazione predefinita, se non sono installati prodotti di protezione dalla posta indesiderata o di blocco dei contenuti, i problemi di protezione secondari controllati da tali prodotti vengono automaticamente ignorati e non vengono considerati nello stato di protezione generale. Tuttavia, se un problema di protezione è seguito da un collegamento **Ignora**, è possibile scegliere di ignorare il problema se si è certi di non avere la necessità di risolverlo. Se si decide in un secondo momento di risolvere un problema precedentemente ignorato, è possibile includerlo nello stato della protezione perché venga rilevato.

Configurazione dei problemi ignorati

È possibile indicare nello stato di protezione generale del computer di includere o escludere dal rilevamento determinati problemi. Se un problema di protezione è seguito da un collegamento **Ignora** , è possibile scegliere di ignorare il problema se si è certi di non avere la necessità di risolverlo. Se si decide in un secondo momento di risolvere un problema precedentemente ignorato, è possibile includerlo nello stato della protezione perché venga rilevato.

Per configurare i problemi ignorati

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto a **Stato della protezione** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. Nel riquadro Problemi ignorati, eseguire una delle seguenti operazioni:
   - Per includere problemi precedentemente ignorati nello stato della protezione, deselezionare le relative caselle di controllo.
   - Per escludere dei problemi dallo stato della protezione, selezionare le relative caselle di controllo.
4. Fare clic su **OK**.

Configurazione delle opzioni utente

Se si utilizzano programmi McAfee che richiedono autorizzazioni utente, tali autorizzazioni corrispondono per impostazione predefinita agli account utente di Windows del computer in uso. Per facilitare la gestione di questi programmi da parte degli utenti, è possibile decidere in qualsiasi momento di utilizzare gli account utente McAfee.

Se si decide di utilizzare gli account utente McAfee, eventuali nomi utente e autorizzazioni già esistenti nel programma per il controllo genitori in uso verranno importati automaticamente. Tuttavia, prima di utilizzare gli account utente McAfee, è necessario creare un account Amministratore. In seguito sarà possibile creare e configurare altri account utente McAfee.

Utilizzo degli account utente McAfee

Per impostazione predefinita, si utilizzano gli account utente di Windows. Tuttavia, l'utilizzo degli account utente McAfee rende superflua la creazione di nuovi account utente di Windows.

Per utilizzare gli account utente McAfee

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto a **Utenti** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. Per utilizzare gli account utente McAfee, fare clic su **Passa a**.

Se si utilizzano gli account utente McAfee per la prima volta, è necessario **procedere alla creazione di un account** Amministratore (pagina 23).

Creazione di un account Amministratore

La prima volta che si utilizzano gli account utente McAfee, viene richiesta la creazione di un account Amministratore.

Per creare un account Amministratore

1. Immettere una password nella casella **Password** e immetterla nuovamente nella casella **Conferma password**.
2. Selezionare una domanda per il recupero della password dall'elenco fornito e immettere la risposta nella casella **Risposta**.
3. Fare clic su **Applica**.

   Al termine della procedura, il tipo di account utente viene aggiornato nel riquadro in cui sono visualizzati gli account utente e le autorizzazioni del programma per il controllo genitori preesistente, se presenti. Se si configurano gli

account utente per la prima volta, verrà visualizzato il riquadro di gestione utente.

Configurazione delle opzioni utente

Se si decide di utilizzare gli account utente McAfee, eventuali nomi utente e autorizzazioni già esistenti nel programma per il controllo genitori in uso verranno importati automaticamente. Tuttavia, prima di utilizzare gli account utente McAfee, è necessario creare un account Amministratore. In seguito sarà possibile creare e configurare altri account utente McAfee.

Per configurare le opzioni utente

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto a **Utenti** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. In **Account utente** fare clic su **Aggiungi**.
4. Immettere un nome utente nella casella **Nome utente**.
5. Immettere una password nella casella **Password** e immetterla nuovamente nella casella **Conferma password**.
6. Selezionare la casella di controllo **Utente di avvio** se si desidera che il nuovo utente si colleghi automaticamente all'avvio di SecurityCenter.
7. In **Tipo account utente**, selezionare il tipo di account dell'utente e fare clic su **Crea**.

Nota: dopo aver creato l'account utente, è necessario configurare le impostazioni di utente con limitazioni in Controllo genitori.

8. Per modificare la password, l'accesso automatico o il tipo di account di un utente, selezionare il nome dell'utente dall'elenco e fare clic su **Modifica**.
9. Al termine dell'operazione, fare clic su **Applica**.

Recupero della password di amministratore

Se si dimentica la password di amministratore, è possibile recuperarla.

Per recuperare la password di amministratore

1 Fare clic con il pulsante destro del mouse sull'icona M di SecurityCenter, quindi fare clic su **Cambia utente**.

2 Nell'elenco **Nome utente** selezionare **Amministratore**, quindi fare clic su **Password dimenticata**.

3 Immettere la risposta alla domanda segreta selezionata al momento della creazione dell'account Amministratore.

4 Fare clic su **Invia**.

   Verrà visualizzata la password di amministratore dimenticata.

Modifica della password di amministratore

Se si ritiene che la password di amministratore sia compromessa o si hanno difficoltà a ricordarla, è possibile modificarla.

Per modificare la password di amministratore

1 Fare clic con il pulsante destro del mouse sull'icona M di SecurityCenter, quindi fare clic su **Cambia utente**.

2 Nell'elenco **Nome utente** selezionare **Amministratore**, quindi fare clic su **Modifica password**.

3 Immettere la password in uso nella casella **Vecchia password**
   .

4 Immettere la nuova password nella casella **Password** e immetterla nuovamente nella casella **Conferma password**.

5 Fare clic su **OK**.

Configurazione delle opzioni di aggiornamento

Quando si è connessi a Internet, SecurityCenter verifica automaticamente ogni quattro ore la disponibilità di aggiornamenti per tutti i servizi McAfee in uso, quindi installa gli aggiornamenti più recenti dei prodotti. È tuttavia sempre possibile verificare manualmente la presenza di aggiornamenti mediante l'icona di SecurityCenter situata nell'area di notifica, all'estremità destra della barra delle applicazioni.

Verifica automatica degli aggiornamenti

Quando si è connessi a Internet, SecurityCenter verifica automaticamente la disponibilità di aggiornamenti ogni quattro ore. È tuttavia possibile configurare SecurityCenter in modo tale che visualizzi una notifica prima di scaricare o installare gli aggiornamenti.

Per verificare automaticamente la disponibilità di aggiornamenti

1 In **Informazioni su SecurityCenter**, fare clic su **Configura**.

2 Fare clic sulla freccia accanto allo stato **Gli aggiornamenti automatici sono attivi** per ingrandire il riquadro, quindi fare clic su **Avanzate**.

3 Selezionare un'opzione nel riquadro Opzioni di aggiornamento:

- **Installa automaticamente gli aggiornamenti e avvisa quando il prodotto viene aggiornato (consigliato)** (pagina 27)
- **Scarica automaticamente gli aggiornamenti e avvisa quando sono pronti per l'installazione** (pagina 28)
- **Avvisa prima di scaricare aggiornamenti** (pagina 28)

4 Fare clic su **OK**.

Nota: per una protezione ottimale, McAfee consiglia di configurare SecurityCenter in modo tale da eseguire automaticamente la ricerca e l'installazione degli aggiornamenti. Se tuttavia si desidera aggiornare manualmente i servizi di protezione, è possibile **disattivare l'aggiornamento automatico** (pagina 29).

Esecuzione automatica del download e dell'installazione degli aggiornamenti

Se si seleziona **Installa automaticamente gli aggiornamenti e avvisa quando i servizi vengono aggiornati (consigliato)** nel riquadro Opzioni di aggiornamento di SecurityCenter, il download e l'installazione degli aggiornamenti verranno eseguiti automaticamente.

Download automatico degli aggiornamenti

Se si seleziona **Scarica automaticamente gli aggiornamenti e avvisa quando sono pronti per l'installazione** nel riquadro Opzioni di aggiornamento, SecurityCenter scarica automaticamente gli aggiornamenti e avvisa quando un aggiornamento è pronto per l'installazione. È quindi possibile decidere di installare o **posticipare l'aggiornamento** (pagina 29).

Per installare un aggiornamento scaricato automaticamente

1. Fare clic su **Aggiorna i prodotti adesso** nella finestra dell'avviso e fare clic su **OK**.

   Se richiesto, è necessario connettersi al sito Web per verificare l'abbonamento prima di effettuare il download.

2. Una volta verificato l'abbonamento, fare clic su **Aggiorna** nel riquadro Aggiornamenti per scaricare e installare l'aggiornamento. Se l'abbonamento è scaduto, fare clic su **Rinnova abbonamento** nella finestra dell'avviso e attenersi alle istruzioni visualizzate.

Nota: in alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutti i programmi prima di riavviare.

Avvisa prima di scaricare aggiornamenti

Se si seleziona **Avvisa prima di scaricare aggiornamenti** nel riquadro Opzioni di aggiornamento, prima del download di eventuali aggiornamenti verrà visualizzato un avviso di SecurityCenter. Sarà quindi possibile decidere di scaricare e installare un aggiornamento dei servizi di protezione per rimuovere la minaccia di un attacco.

Per scaricare e installare un aggiornamento

1. Selezionare **Aggiorna i prodotti adesso** nella finestra dell'avviso e fare clic su **OK**.

2. Se richiesto, accedere al sito Web.

   L'aggiornamento viene scaricato automaticamente.

3. Al termine dell'installazione dell'aggiornamento fare clic su **OK**.

Nota: in alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutti i programmi prima di riavviare.

Disattivazione dell'aggiornamento automatico

Per una protezione ottimale, McAfee consiglia di configurare SecurityCenter in modo tale da eseguire automaticamente la ricerca e l'installazione degli aggiornamenti. Se tuttavia si desidera aggiornare manualmente i servizi di protezione, è possibile disattivare l'aggiornamento automatico.

Nota: è necessario ricordarsi di **verificare manualmente la disponibilità di aggiornamenti** (pagina 30) almeno una volta alla settimana. Se non si effettua tale verifica, il computer non disporrà degli aggiornamenti di protezione più recenti.

Per disattivare l'aggiornamento automatico

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto allo stato **Gli aggiornamenti automatici sono attivi** per ingrandire il riquadro.
3. Fare clic su **Disattiva**.
4. Fare clic su **Sì** per confermare la modifica.

   Lo stato viene aggiornato nell'intestazione.

Se per sette giorni non viene eseguita la ricerca manuale degli aggiornamenti, verrà visualizzato un avviso che ricorda di ricercare gli aggiornamenti.

Posticipazione degli aggiornamenti

Se non si ha tempo di aggiornare i servizi di protezione quando viene visualizzato l'avviso, è possibile decidere di visualizzare l'avviso in seguito o di ignorare l'avviso.

Per posticipare un aggiornamento

- Effettuare una delle seguenti operazioni:
  - Selezionare **Visualizza un promemoria in un secondo momento** nella finestra dell'avviso e fare clic su **OK**.
  - Selezionare **Chiudere l'avviso** e fare clic su **OK** per chiudere la finestra dell'avviso senza intraprendere alcuna azione.

Verifica manuale degli aggiornamenti

Quando si è connessi a Internet, SecurityCenter verifica automaticamente la disponibilità di aggiornamenti ogni quattro ore, quindi installa gli aggiornamenti dei prodotti più recenti. È tuttavia sempre possibile verificare manualmente la presenza di aggiornamenti mediante l'icona di SecurityCenter nell'area di notifica di Windows, posta all'estremità destra della barra delle applicazioni.

Nota: per una protezione ottimale, McAfee consiglia di configurare SecurityCenter in modo tale da eseguire automaticamente la ricerca e l'installazione degli aggiornamenti. Se tuttavia si desidera aggiornare manualmente i servizi di protezione, è possibile **disattivare l'aggiornamento automatico** (pagina 29).

Per verificare manualmente la disponibilità di aggiornamenti

1. Assicurarsi che il computer sia connesso a Internet.
2. Fare clic con il pulsante destro del mouse sull'icona M di SecurityCenter nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni, quindi scegliere **Aggiornamenti**.

   Mentre SecurityCenter verifica la disponibilità di aggiornamenti, è possibile proseguire con altre attività.

   Per maggiore praticità, nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni, viene visualizzata un'icona animata. Quando SecurityCenter ha terminato l'operazione di verifica, l'icona scompare automaticamente.
3. Se richiesto, accedere al sito Web per verificare il proprio abbonamento.

Nota: in alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutti i programmi prima di riavviare.

Configurazione delle opzioni di avviso

SecurityCenter informa automaticamente l'utente, mediante avvisi e riproduzione di suoni, della diffusione di virus, di minacce per la protezione e degli aggiornamenti dei prodotti. È tuttavia possibile configurare SecurityCenter in modo da visualizzare solo gli avvisi che richiedono un'attenzione immediata.

Configurazione delle opzioni di avviso

SecurityCenter informa automaticamente l'utente, mediante avvisi e riproduzione di suoni, della diffusione di virus, di minacce per la protezione e degli aggiornamenti dei prodotti. È tuttavia possibile configurare SecurityCenter in modo da visualizzare solo gli avvisi che richiedono un'attenzione immediata.

Per configurare le opzioni di avviso

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto ad **Avvisi** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. Selezionare una delle seguenti opzioni nel riquadro Opzioni di avviso:
   - **Avvisa quando si verifica la diffusione di un virus o una minaccia per la protezione**
   - **Visualizza avvisi informativi quando viene rilevata la modalità di gioco**
   - **Riproduci un suono quando si verifica un avviso.**
   - **Mostra schermata iniziale di McAfee all'avvio di Windows**
4. Fare clic su **OK**.

Nota: per disattivare gli avvisi informativi futuri dall'avviso visualizzato, selezionare la casella di controllo **Non visualizzare più questo messaggio**. Sarà possibile riattivare gli avvisi in un secondo tempo dal riquadro Avvisi informativi.

Configurazione degli avvisi informativi

Gli avvisi informativi avvertono l'utente del verificarsi di eventi che non richiedono una risposta immediata. Se si disattivano gli avvisi informativi futuri dall'avviso stesso, è possibile riattivarli in seguito dal riquadro degli avvisi informativi.

Per configurare gli avvisi informativi

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto ad **Avvisi** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. In **Configurazione di SecurityCenter**, fare clic su **Avvisi informativi**.
4. Deselezionare la casella di controllo **Nascondi avvisi informativi**, quindi deselezionare le caselle di controllo corrispondenti agli avvisi che si desidera visualizzare.
5. Fare clic su **OK**.

CAPITOLO 5

Esecuzione delle attività comuni

È possibile eseguire attività comuni come il ritorno al riquadro Home, la visualizzazione degli eventi più recenti, la gestione della rete di computer (nel caso in cui si tratti di un computer con capacità di gestione della rete), nonché la manutenzione del computer. Se è stato installato McAfee Data Backup, è anche possibile eseguire il backup dei dati.

In questo capitolo

Esecuzione delle attività comuni

È possibile eseguire attività comuni come il ritorno al riquadro Home, la visualizzazione degli eventi più recenti, la manutenzione del computer, la gestione della rete (nel caso in cui si tratti di un computer con capacità di gestione della rete) e il backup dei dati, se è stato installato McAfee Data Backup.

Per eseguire le attività comuni

- In **Attività comuni** nel menu standard, eseguire una delle seguenti operazioni:
  - Per ritornare al riquadro Home, fare clic su **Home**.
  - Per visualizzare gli eventi recenti rilevati dal software di protezione, fare clic su **Eventi recenti**.
  - Per eliminare file inutilizzati, deframmentare i dati e ripristinare le impostazioni precedenti del computer, fare clic su **Manutenzione computer**.
  - Se il computer dispone di capacità di gestione delle reti, fare clic su **Gestione rete** per gestire la rete di computer.

    Network Manager esegue il monitoraggio dei computer in rete alla ricerca di possibili vulnerabilità nella protezione, consentendo di individuare eventuali problemi di protezione della rete.

- Per creare delle copie di backup dei file, se è stato installato McAfee Data Backup fare clic su **Backup dati**.

  Il backup automatizzato salva copie dei file più importanti nelle posizioni desiderate, crittografandoli e memorizzandoli su CD/DVD o su unità USB, esterne o di rete.

Suggerimento: per comodità, è possibile eseguire le attività comuni da altre due posizioni, da **Home** nel menu avanzato e dal menu **Collegamenti rapidi** dell'icona M di SecurityCenter all'estremità destra della barra delle applicazioni. È inoltre possibile visualizzare gli eventi recenti e i registri completi per tipo in **Rapporti e registri** nel menu avanzato.

Visualizzazione degli eventi recenti

Gli eventi recenti vengono registrati quando si verificano cambiamenti nel computer, ad esempio quando si attiva o disattiva un tipo di protezione, si rimuove una minaccia o viene bloccato un tentativo di connessione via Internet. È possibile visualizzare i 20 eventi più recenti con i relativi dettagli.

Per ulteriori dettagli sugli eventi relativi a un particolare prodotto, consultare la guida in linea del prodotto.

Per visualizzare gli eventi recenti

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Visualizza eventi recenti**.

   Gli eventi recenti vengono visualizzati nell'elenco, insieme alla data e a una breve descrizione.

2. Selezionare un evento da **Eventi recenti** per visualizzarne le informazioni nel riquadro dei dettagli.

   Le azioni consentite vengono visualizzate nella sezione **Desidero**.

3. Per visualizzare un elenco di eventi più completo, fare clic su **Visualizza registro**.

Manutenzione automatica del computer

Per liberare spazio su disco e ottimizzare le prestazioni del computer, è possibile programmare le attività di QuickClean o di deframmentazione dischi ad intervalli regolari. Queste attività comprendono l'eliminazione, la distruzione e la deframmentazione di file e cartelle.

Per eseguire la manutenzione automatica del computer:

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Manutenzione computer**.
2. In **Pianificazione attività**, fare clic su **Avvia**.
3. Nell'elenco delle operazioni, selezionare **QuickClean** o **Deframmentazione dischi**.
4. Effettuare una delle seguenti operazioni:
   - Per modificare un'attività esistente, selezionarla e fare clic su **Modifica**. Seguire le istruzioni riportate sullo schermo.
   - Per creare una nuova attività, immettere il nome nella casella **Nome attività**, quindi fare clic su **Crea**. Seguire le istruzioni riportate sullo schermo.
   - Per eliminare un'attività, selezionarla e fare clic su **Elimina**.
5. In **Riepilogo attività**, verificare la data dell'ultima esecuzione dell'attività, la data della prossima esecuzione e lo stato.

Manutenzione manuale del computer

È possibile eseguire manualmente le attività di manutenzione per eliminare i file inutilizzati, deframmentare i dati oppure per ripristinare le precedenti impostazioni del computer.

Per eseguire la manutenzione manuale del computer

- Effettuare una delle seguenti operazioni:
  - Per utilizzare QuickClean, fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi**, fare clic su **Manutenzione computer** e quindi su **Avvia**.
  - Per utilizzare Deframmentazione dischi, fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi**, fare clic su **Manutenzione computer** e quindi su **Analizza**.
  - Per utilizzare l'utilità di ripristino del sistema, selezionare **Strumenti** dal menu avanzato, fare clic su **Ripristino configurazione di sistema**, quindi su **Avvia**.

Rimozione di file e cartelle non utilizzati

Utilizzare QuickClean per liberare spazio su disco e ottimizzare le prestazioni del computer.

Per rimuovere file e cartelle non utilizzati

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Manutenzione computer**.
2. In **QuickClean** fare clic su **Avvia**.
3. Seguire le istruzioni riportate sullo schermo.

Deframmentazione di file e cartelle

La frammentazione dei file si verifica quando si eliminano file e cartelle e si aggiungono nuovi file. La frammentazione rallenta l'accesso al disco e riduce le prestazioni del computer, sebbene spesso non in modo significativo.

L'utilità di deframmentazione consente di riscrivere parti di un file in settori adiacenti del disco rigido per aumentare la velocità di accesso e di recupero.

Per deframmentare file e cartelle

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Manutenzione computer**.
2. In **Deframmentazione dischi**, fare clic su **Analizza**.
3. Seguire le istruzioni riportate sullo schermo.

Ripristino delle impostazioni precedenti del computer

I punti di ripristino sono istantanee del computer che Windows salva periodicamente e quando si verificano eventi importanti, ad esempio quando si installa un programma o un driver. È tuttavia possibile creare e denominare i propri punti di ripristino in qualsiasi momento.

Utilizzare i punti di ripristino per annullare modifiche potenzialmente pericolose per il computer e ritornare alle impostazioni precedenti.

Per ripristinare le impostazioni precedenti del computer

1. Nel menu avanzato, fare clic su **Strumenti**, quindi su **Ripristino configurazione di sistema**.
2. In **Ripristino configurazione di sistema**, fare clic su **Avvia**.
3. Seguire le istruzioni riportate sullo schermo.

Gestione della rete

Se il computer dispone delle capacità di gestione della rete di computer, è possibile utilizzare Network Manager per monitorare i computer in rete alla ricerca di eventuali vulnerabilità nella protezione, in modo tale da consentire l'identificazione dei problemi.

Se lo stato della protezione del computer non è monitorato sulla rete, ciò significa che il computer non fa parte della rete oppure è un membro non gestito della rete. Per ulteriori dettagli, consultare il file della guida in linea di Network Manager.

Per gestire la rete

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Gestione rete**.
2. Fare clic sull'icona che rappresenta il computer nella mappa della rete.
3. Nella sezione **Desidero**, fare clic su **Monitorare il computer**.

Ulteriori informazioni sui virus

Utilizzare la Libreria di informazioni sui virus e la Virus Map per:

- Ottenere ulteriori informazioni su virus, messaggi di posta elettronica ingannevoli (hoax) e altre minacce più recenti.
- Ottenere strumenti gratuiti per la rimozione dei virus che facilitano la riparazione del computer.
- Ottenere una panoramica in tempo reale degli ultimi virus in circolazione a livello mondiale.

Per ottenere ulteriori informazioni sui virus

1. Nel menu avanzato, fare clic su **Strumenti**, quindi su **Informazioni sui virus**.
2. Effettuare una delle seguenti operazioni:
   - Ricercare i virus utilizzando la Libreria di informazioni sui virus gratuita di McAfee.
   - Ricercare i virus utilizzando la World Virus Map sul sito web di McAfee.

CAPITOLO 6

McAfee QuickClean

Durante la navigazione in Internet, sul computer si accumulano rapidamente file e dati inutili. QuickClean permette di proteggere la privacy e di eliminare i file superflui relativi a Internet e posta elettronica, identificando ed eliminando i file accumulati durante la navigazione, compresi i cookie, la posta elettronica, i download e la cronologia: file che possono contenere dati personali. QuickClean protegge la privacy assicurando l'eliminazione in modalità protetta delle informazioni riservate.

QuickClean consente inoltre di eliminare i programmi indesiderati, specificando i file da eliminare e rimuovendo i file non necessari, senza rimuovere le informazioni indispensabili.

In questo capitolo

Informazioni sulle funzioni di QuickClean

Questa sezione descrive le funzioni di QuickClean.

Funzioni

McAfee QuickClean fornisce un insieme di strumenti efficaci e facili da usare per rimuovere in modo sicuro i file non più necessari. È così possibile liberare prezioso spazio su disco e ottimizzare le prestazioni del computer.

CAPITOLO 7

Pulizia del computer

QuickClean consente di eliminare file e cartelle in tutta sicurezza.

Quando si naviga in Internet, il browser copia ciascuna pagina Internet e la grafica associata in una cartella cache sul disco, in modo da poterla poi caricare rapidamente in caso di nuova visita. La memorizzazione di file nella cache è utile se si visitano ripetutamente le stesse pagine Internet e il relativo contenuto non viene modificato di frequente. Quasi sempre, tuttavia, i file memorizzati nella cache sono inutili e quindi eliminabili.

È possibile eliminare diversi elementi mediante le operazioni di pulitura riportate di seguito.

- Pulitura del Cestino: esegue la pulitura del Cestino di Windows.
- Pulitura dei file temporanei: elimina i file memorizzati in cartelle temporanee.
- Pulitura dei collegamenti: elimina i collegamenti interrotti e quelli non associati a programmi.
- Pulitura dei frammenti di file persi: elimina dal computer i frammenti di file persi.
- Pulitura del registro di sistema: elimina le informazioni del registro di sistema di Windows relative ai programmi che non sono più installati nel computer.
- Pulitura della cache: elimina i file memorizzati nella cache accumulati durante la navigazione in Internet. I file di questo tipo vengono solitamente memorizzati come file temporanei di Internet.
- Pulitura dei cookie: elimina i cookie. I file di questo tipo vengono solitamente memorizzati come file temporanei di Internet.
  I cookie sono piccoli file che il browser Web registra sul computer in seguito alla richiesta di un server Web. Ogni volta che sul server Web viene visualizzata una pagina Web, il browser invia di nuovo il cookie al server. I cookie svolgono una funzione simile quella di un cartellino che consente al server Web di registrare quali pagine vengono visualizzate e con quale frequenza.
- Pulitura della cronologia del browser: elimina la cronologia del browser.
- Pulitura della posta di Outlook Express e Outlook (per posta eliminata e inviata): elimina la posta elettronica dalle cartelle Posta inviata e Posta eliminata di Outlook.

- Pulitura dei file utilizzati di recente: elimina i file utilizzati di recente e memorizzati sul computer, ad esempio i documenti di Microsoft Office.
- Pulitura di ActiveX e plug-in: elimina i controlli ActiveX e i plug-in.
  ActiveX è una tecnologia utilizzata per implementare controlli all'interno di un programma. Un controllo ActiveX è in grado di aggiungere un pulsante all'interfaccia di un programma. La maggior parte di questi controlli è innocua, tuttavia la tecnologia ActiveX potrebbe essere utilizzata per acquisire informazioni dal computer.
  I plug-in sono piccoli programmi software che si inseriscono in applicazioni di dimensioni maggiori per offrire ulteriori funzioni. I plug-in consentono al browser Web di accedere ai file incorporati nei documenti HTML il cui formato non verrebbe normalmente riconosciuto (ad esempio, file di animazione, audio e video) e, quindi, di eseguirli.
- Pulitura dei punti di ripristino configurazione di sistema: elimina dal computer i punti di ripristino configurazione di sistema obsoleti.

In questo capitolo

Uso di QuickClean

Questa sezione descrive come utilizzare QuickClean.

Pulitura del computer

È possibile eliminare file e cartelle inutilizzati, liberare spazio su disco e migliorare le prestazioni del computer.

Per eseguire la pulitura del computer:

1 Nel menu avanzato, fare clic su **Strumenti**.

2 Fare clic su **Manutenzione computer**, quindi su **Avvia** in **McAfee QuickClean**.

3 Effettuare una delle seguenti operazioni:

- Scegliere **Avanti** per accettare le operazioni di pulitura predefinite visualizzate nell'elenco.
- Selezionare o deselezionare le operazioni di pulitura appropriate e fare clic su **Avanti.** Per la pulitura dei file utilizzati di recente, è possibile fare clic su **Proprietà** per deselezionare i programmi i cui elenchi non verranno puliti.
- Fare clic su **Ripristina impostazioni predefinite** per ripristinare le operazioni di pulitura predefinite, quindi su **Avanti**.

4 Al termine dell'analisi, scegliere **Avanti** per confermare l'eliminazione dei file. È possibile espandere questo elenco per visualizzare i file di cui verrà eseguita la pulitura con il relativo percorso.

5 Fare clic su **Avanti**.

6 Effettuare una delle seguenti operazioni:

- Fare clic su **Avanti** per accettare l'opzione predefinita **Eliminare i file usando l'eliminazione standard di Windows**.
- Fare clic su **Eliminare i file in modalità protetta utilizzando Shredder** e specificare il numero di tentativi. Non è possibile recuperare i file eliminati con Shredder.

7 Scegliere **Fine**.

8 In **Riepilogo di QuickClean**, è visualizzato il numero di file del registro di sistema eliminati e la quantità di spazio su disco recuperato dopo la pulitura Internet e del disco.

CAPITOLO 8

McAfee Shredder

I file eliminati possono essere recuperati dal computer anche dopo che il Cestino è stato svuotato. Quando si elimina un file, lo spazio occupato sull'unità disco viene contrassegnato da Windows come non più in uso, ma il file fisicamente esiste ancora. Grazie all'utilizzo di appositi strumenti informatici, è possibile recuperare dichiarazioni dei redditi, curricula professionali o altri documenti eliminati. Shredder protegge la privacy dell'utente eliminando in modo sicuro e definitivo i file indesiderati.

Per eliminare definitivamente un file, occorre sovrascriverlo ripetutamente con nuovi dati. Microsoft® Windows non elimina i file in modo sicuro in quanto ogni operazione sui file risulterebbe molto lenta. La distruzione di un documento non ne impedisce sempre il recupero poiché alcuni programmi creano copie temporanee nascoste dei documenti aperti. Se si distruggono solo i documenti visibili in Esplora risorse di Windows®, è possibile che ne esistano ancora delle copie temporanee.

Nota: il backup dei file distrutti non viene eseguito, pertanto non sarà possibile ripristinare i file eliminati da Shredder.

In questo capitolo

Informazioni sulle funzioni di Shredder

Questa sezione illustra le funzioni di Shredder.

Funzioni

Shredder consente di cancellare il contenuto del Cestino, i file temporanei di Internet, la cronologia dei siti Web, file, cartelle e dischi.

CAPITOLO 9

Cancellazione dei file indesiderati con Shredder

Shredder protegge la privacy del'utente eliminando in modo sicuro e definitivo i file indesiderati, ad esempio il contenuto del Cestino, i file temporanei di Internet e la cronologia dei siti Web. È possibile selezionare i file e le cartelle da distruggere oppure eseguire una ricerca.

In questo capitolo

Uso di Shredder

Questa sezione descrive le modalità di utilizzo di Shredder.

Distruzione di file, cartelle e dischi

I file possono continuare a risiedere nel computer anche dopo aver svuotato il Cestino. Tuttavia, una volta distrutti, i dati risultano definitivamente eliminati e gli hacker non possono accedervi.

Per distruggere file, cartelle e dischi:

1. Nel menu avanzato, fare clic su **Strumenti**, quindi su **Shredder**.
2. Effettuare una delle seguenti operazioni:
   - Fare clic su **Cancellare file e cartelle** per distruggere file e cartelle.
   - Fare clic su **Cancellare un intero disco** per distruggere il contenuto di un intero disco.
3. Selezionare uno dei seguenti livelli di distruzione:
   - **Rapido**: distrugge gli elementi selezionati utilizzando 1 solo passaggio.
   - **Completo**: distrugge gli elementi selezionati utilizzando 7 passaggi.
   - **Personalizzato**: distrugge gli elementi selezionati utilizzando 10 passaggi. Un numero più elevato di passaggi nel processo di distruzione rende più sicura l'eliminazione dei file.
4. Fare clic su **Avanti**.
5. Effettuare una delle seguenti operazioni:
   - Se si desidera distruggere file, fare clic su **Contenuto del Cestino**, **File temporanei Internet** o **Cronologia siti Web** nell'elenco **Selezionare i file da distruggere**. Se invece si desidera distruggere il contenuto di un disco, fare clic su di esso.
   - Fare clic su **Sfoglia**, individuare i file da distruggere e selezionarli.
   - Digitare il percorso dei file da distruggere nell'elenco **Selezionare i file da distruggere**.
6. Fare clic su **Avanti**.
7. Fare clic su **Fine** per completare l'operazione.
8. Fare clic su **Fine**.

C A P I T O L O 1 0

McAfee Network Manager

McAfee® Network Manager rappresenta graficamente i computer e i componenti che costituiscono la rete domestica. Network Manager consente di eseguire il monitoraggio remoto dello stato di protezione di tutti i computer gestiti in rete e quindi di risolvere le vulnerabilità della protezione segnalate su di essi.

Prima di iniziare a utilizzare Network Manager, è possibile conoscerne alcune delle funzioni più comuni. La guida di Network Manager contiene dettagli sulla configurazione e sull'utilizzo di tali funzioni.

In questo capitolo

Funzioni

Network Manager offre le seguenti funzioni:

Mappa grafica della rete

La mappa della rete di Network Manager fornisce una panoramica grafica dello stato di protezione dei computer e dei componenti che costituiscono la rete domestica. Quando vengono apportate modifiche alla rete, ad esempio con l'aggiunta di un computer, la mappa della rete è in grado di riconoscerle. È possibile aggiornare la mappa della rete, rinominare la rete e mostrare o nascondere i componenti della mappa per personalizzare la visualizzazione. Possono inoltre essere visualizzati i dettagli associati a uno qualsiasi dei componenti mostrati sulla mappa della rete.

Gestione remota

Utilizzare la mappa della rete di Network Manager per gestire lo stato di protezione dei computer che costituiscono la rete domestica. È possibile invitare un computer a diventare membro della rete gestita, monitorare lo stato di protezione del computer gestito e risolvere le vulnerabilità conosciute della protezione da un computer remoto della rete.

Informazioni sulle icone di Network Manager

Nella seguente tabella sono descritte le icone di uso comune nella mappa della rete di Network Manager.

Icona	Descrizione
	Rappresenta un computer gestito in linea
	Rappresenta un computer gestito non in linea
	Rappresenta un computer non gestito su cui è installato il software di protezione McAfee 2007
	Rappresenta un computer non gestito e non in linea
	Rappresenta un computer in linea su cui non è installato il software di protezione McAfee 2007 oppure un dispositivo di rete sconosciuto
	Rappresenta un computer non in linea su cui non è installato il software di protezione McAfee 2007 oppure un dispositivo di rete sconosciuto e non in linea
	Indica che l'elemento corrispondente è protetto e connesso
	Indica che l'elemento corrispondente richiede l'attenzione dell'utente
	Indica che l'elemento corrispondente richiede l'attenzione dell'utente ed è disconnesso
	Rappresenta un router domestico senza fili
	Rappresenta un router domestico standard
	Rappresenta Internet, quando è stata effettuata la connessione
	Rappresenta Internet, quando non è stata effettuata la connessione

CAPITOLO 11

Impostazione di una rete gestita

Per impostare una rete gestita occorre organizzare gli elementi della mappa della rete e aggiungere membri (computer) alla rete.

In questo capitolo

Utilizzo della mappa della rete

Ogni volta che un computer si connette alla rete, Network Manager analizza lo stato della rete al fine di determinare se sono presenti eventuali membri (gestiti o non gestiti), gli attributi del router e lo stato di Internet. Se non viene rilevato alcun membro, Network Manager presume che il computer attualmente connesso sia il primo della rete, rendendolo automaticamente membro gestito con autorizzazioni di amministratore. Per impostazione predefinita, il nome della rete include il gruppo di lavoro o nome di dominio del primo computer che si connette alla rete e su cui è installato il software di protezione McAfee 2007. Tuttavia, è possibile rinominare la rete in qualsiasi momento.

Quando si apportano modifiche alla propria rete (ad esempio, mediante l'aggiunta di un computer), è possibile personalizzare la mappa della rete. Ad esempio, è possibile aggiornare la mappa della rete, rinominare la rete e mostrare o nascondere i componenti della mappa della rete per personalizzare la visualizzazione. Possono inoltre essere visualizzati i dettagli associati a uno qualsiasi dei componenti mostrati sulla mappa della rete.

Accesso alla mappa della rete

Per accedere alla mappa della propria rete occorre avviare Network Manager dall'elenco delle attività comuni di SecurityCenter. La mappa della rete rappresenta graficamente i computer e i componenti che costituiscono la rete domestica.

Per accedere alla mappa della rete:

- Nel Menu standard o nel Menu avanzato, fare clic su **Gestione rete**.
  La mappa della rete viene visualizzata nel riquadro a destra.

Nota: Al primo accesso alla mappa della rete, prima della visualizzazione della mappa viene richiesto di impostare come affidabili gli altri computer della rete.

Aggiornamento della mappa della rete

È possibile aggiornare la mappa della rete in qualsiasi momento; ad esempio, dopo che un nuovo computer è diventato membro della rete gestita.

Per aggiornare la mappa della rete:

1. Nel Menu standard o nel Menu avanzato, fare clic su **Gestione rete**.
   La mappa della rete viene visualizzata nel riquadro a destra.
2. Fare clic su **Aggiornare la mappa della rete** nella sezione **Desidero**.

Nota: il collegamento **Aggiornare la mappa della rete** è disponibile solo quando non è stato selezionato alcun elemento nella mappa della rete. Per deselezionare un elemento, fare clic sull'elemento selezionato oppure in un'area vuota della mappa della rete.

Ridenominazione della rete

Per impostazione predefinita, il nome della rete include il gruppo di lavoro o nome di dominio del primo computer che si connette alla rete e su cui è installato il software di protezione McAfee 2007. Se il nome non è appropriato è possibile modificarlo.

Per rinominare la rete:

1. Nel Menu standard o nel Menu avanzato, fare clic su **Gestione rete**.
   La mappa della rete viene visualizzata nel riquadro a destra.
2. Fare clic su **Rinominare la rete** nella sezione **Desidero**.
3. Digitare il nome della rete nella casella **Rinomina rete**.
4. Fare clic su **OK**.

Nota: il collegamento **Rinomina rete** è disponibile solo quando non è stato selezionato alcun elemento nella mappa della rete. Per deselezionare un elemento, fare clic sull'elemento selezionato oppure in un'area vuota della mappa della rete.

Visualizzazione o non visualizzazione di elementi sulla mappa della rete

Per impostazione predefinita, nella mappa della rete sono visualizzati tutti i computer e i componenti della rete domestica. Tuttavia, se vi sono elementi nascosti, è possibile visualizzarli in qualsiasi momento. È possibile nascondere solo gli elementi non gestiti, ma non i computer gestiti.

Per...	Nel Menu standard o nel Menu avanzato, fare clic su **Gestione rete**, quindi eseguire una delle seguenti operazioni.
Nascondere un elemento sulla mappa della rete	Fare clic su un elemento sulla mappa della rete, quindi su **Nascondere l'elemento** nella sezione **Desidero**. Nella finestra di dialogo di conferma, fare clic su **Sì**.
Mostrare elementi nascosti sulla mappa della rete	Nella sezione **Desidero**, fare clic su **Visualizzare gli elementi nascosti**.

Visualizzazione dei dettagli di un elemento

Per visualizzare informazioni dettagliate su qualsiasi componente in rete, selezionarne uno nella mappa della rete. Tra le informazioni disponibili sono inclusi il nome del componente, il relativo stato di protezione nonché altri dettagli richiesti per la gestione del componente.

Per visualizzare i dettagli di un elemento:

1. Fare clic sull'icona di un elemento sulla mappa della rete.
2. Nella sezione **Dettagli** è possibile visualizzare le informazioni sull'elemento.

Aggiunta alla rete gestita

Affinché un computer sia gestito in modalità remota oppure ottenga l'autorizzazione per la gestione remota di altri computer in rete, è necessario che diventi membro affidabile della rete. I nuovi computer vengono aggiunti alla rete dai membri della rete (computer) esistenti, dotati di autorizzazioni amministrative. Per garantire che vengano aggiunti alla rete solo i computer affidabili, gli utenti dei computer che concedono l'autorizzazione e quelli che la ricevono devono autenticarsi reciprocamente.

Quando un computer viene aggiunto alla rete, viene richiesto di esporne lo stato di protezione McAfee agli altri computer in rete. Se un computer accetta di esporre il proprio stato di protezione, esso diventerà un membro *gestito* della rete. Se un computer rifiuta di esporre il proprio stato di protezione, esso diventerà un membro *non gestito* della rete. I membri non gestiti della rete sono di solito computer guest che desiderano accedere ad altre funzioni della rete (ad esempio, la condivisione di file o stampanti).

Nota: se sono stati installati altri programmi di rete McAfee (ad esempio, McAfee Wireless Network Security o EasyNetwork), dopo l'aggiunta il computer verrà riconosciuto come computer gestito anche in tali programmi. Il livello di autorizzazione assegnato a un computer in Network Manager si applica a tutti i programmi di rete McAfee. Per ulteriori informazioni sul significato di autorizzazione guest, completa o con autorizzazioni amministrative in altri programmi di rete McAfee, consultare la relativa documentazione.

Aggiunta a una rete gestita

Quando si riceve un invito a diventare membro di una rete gestita, è possibile accettarlo o rifiutarlo. È anche possibile determinare se si desidera che il computer in uso e altri computer in rete eseguano il monitoraggio reciproco delle rispettive impostazioni di protezione (ad esempio, se i servizi di protezione da virus di un computer sono aggiornati).

Per diventare membro di una rete gestita:

1. Nella finestra di dialogo dell'invito, selezionare la casella di controllo **Consenti a questo e ad altri computer della rete di monitorare reciprocamente le rispettive impostazioni di protezione** per consentire ad altri computer della rete gestita di monitorare le impostazioni di protezione del proprio computer.
2. Fare clic su **Aggiungi**.
   Quando si accetta l'invito vengono visualizzate due carte da gioco.
3. Verificare che le carte da gioco siano uguali a quelle visualizzate sul computer che ha inviato l'invito a diventare membro della rete gestita.
4. Fare clic su **Conferma**.

Nota: se sul computer che ha inviato l'invito a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Diventare membro della rete può mettere a rischio il proprio computer; pertanto, fare clic su **Rifiuta** nella finestra di dialogo di conferma.

Invio a un computer di un invito a diventare membro della rete gestita

Se un computer viene aggiunto alla rete gestita oppure un altro computer non gestito è presente in rete, è possibile invitare tale computer a diventare membro della rete gestita. Solo i computer con autorizzazioni amministrative in rete possono invitare altri computer a diventare membri della rete. Quando si invia l'invito, occorre inoltre specificare il livello di autorizzazione che si desidera assegnare al computer aggiunto.

Per invitare un computer a diventare membro della rete gestita:

1. Fare clic sull'icona del computer non gestito nella mappa della rete.
2. Fare clic su **Monitorare il computer** nella sezione **Desidero**.
3. Nella finestra di dialogo Invita un computer a diventare membro della rete gestita, fare clic su una delle seguenti opzioni:
   - **Concedi accesso Guest**
     L'accesso Guest consente al computer di accedere alla rete.
   - **Concedi accesso completo a tutte le applicazioni della rete gestita**
     L'accesso completo (come l'accesso Guest) consente al computer di accedere alla rete.
   - **Concedi accesso con privilegi di amministratore a tutte le applicazioni della rete gestita**
     L'accesso con privilegi di amministratore consente al computer di accedere alla rete con privilegi di amministratore. Consente inoltre al computer di concedere l'accesso ad altri computer che desiderano diventare membri della rete gestita.

4 Fare clic su **Invita**.
Al computer viene inviato un invito a diventare membro della rete gestita. Quando il computer accetta l'invito vengono visualizzate due carte da gioco.

5 Verificare che le carte da gioco siano uguali a quelle visualizzate sul computer invitato a diventare membro della rete gestita.

6 Fare clic su **Consenti accesso**.

Nota: se sul computer invitato a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Consentire al computer di diventare membro della rete può mettere a rischio altri computer; pertanto, fare clic su **Rifiuta accesso** nella finestra di dialogo di conferma.

Impostazione di computer in rete come non affidabili

Se per errore si è accettato di considerare affidabili altri computer in rete, è possibile considerarli come non affidabili.

Per negare l'affidabilità a computer in rete:

- Fare clic su **Non considerare affidabili i computer su questa rete** nella sezione **Desidero**.

Nota: il collegamento **Non considerare affidabili i computer su questa rete** è disponibile solo quando nessun altro computer gestito è diventato membro della rete.

CAPITOLO 12

Gestione remota della rete

Dopo aver impostato la rete gestita, è possibile utilizzare Network Manager per la gestione remota dei computer e dei componenti che costituiscono la rete. È possibile eseguire il monitoraggio dello stato e dei livelli di autorizzazione del computer e dei componenti, nonché risolvere le vulnerabilità della protezione in modalità remota.

In questo capitolo

Monitoraggio dello stato e delle autorizzazioni

Una rete gestita prevede due tipi di membri: membri gestiti e membri non gestiti. I membri gestiti, diversamente da quelli non gestiti, consentono agli altri computer in rete di monitorare lo stato della protezione McAfee. I membri non gestiti sono di solito computer guest che desiderano accedere ad altre funzioni della rete (ad esempio, la condivisione di file o stampanti). Un computer gestito in rete può invitare un computer non gestito a diventare un computer gestito in qualsiasi momento. In maniera simile, un computer gestito può diventare non gestito in qualsiasi momento.

Ai computer gestiti sono associate autorizzazioni amministrative, complete o Guest. Le autorizzazioni amministrative consentono al computer gestito di amministrare lo stato di protezione di tutti gli altri computer gestiti in rete, nonché di concedere agli altri computer di diventare membri della rete. Le autorizzazioni complete e Guest consentono a un computer solo di accedere alla rete. È possibile modificare il livello di autorizzazione di un computer in qualsiasi momento.

Poiché una rete gestita può comprendere anche dei dispositivi (ad esempio i router), è possibile gestire anche questi ultimi mediante Network Manager. È inoltre possibile configurare e modificare le proprietà di visualizzazione di un dispositivo sulla mappa della rete.

Monitoraggio dello stato della protezione di un computer

Se lo stato della protezione del computer non è monitorato sulla rete (perché il computer non è membro della rete oppure è un membro non gestito della rete), è possibile inviare una richiesta di monitoraggio.

Per monitorare lo stato della protezione di un computer:

1. Fare clic sull'icona del computer non gestito nella mappa della rete.
2. Fare clic su **Monitorare il computer** nella sezione **Desidero**.

Interruzione del monitoraggio dello stato della protezione di un computer

È possibile interrompere il monitoraggio dello stato della protezione di un computer gestito nella rete privata, che diventa quindi un computer non gestito.

Per interrompere il monitoraggio dello stato della protezione di un computer:

1. Fare clic sull'icona del computer gestito nella mappa della rete.
2. Fare clic su **Interrompere il monitoraggio del computer** nella sezione **Desidero**.
3. Nella finestra di dialogo di conferma, fare clic su **Sì**.

Modifica delle autorizzazioni di un computer gestito

È possibile modificare le autorizzazioni di un computer gestito in qualsiasi momento. Ciò consente di stabilire quali computer possono monitorare lo stato della protezione (impostazioni di protezione) di altri computer della rete.

Per modificare le autorizzazioni di un computer gestito:

1. Fare clic sull'icona del computer gestito nella mappa della rete.
2. Fare clic su **Modificare i permessi per il computer** nella sezione **Desidero**.
3. Nella finestra di dialogo di modifica dei permessi, selezionare o deselezionare la casella di controllo per determinare se il computer selezionato e altri computer sulla rete gestita possono monitorare reciprocamente il rispettivo stato della protezione.
4. Fare clic su **OK**.

Gestione di una periferica

È possibile gestire una periferica eseguendo l'accesso alla relativa pagina Web di amministrazione in Network Manager.

Per gestire una periferica:

1. Fare clic sull'icona di una periferica nella mappa della rete.
2. Fare clic su **Gestire la periferica** nella sezione **Desidero**.
   Il browser Web verrà aperto e verrà visualizzata la pagina Web di amministrazione della periferica.
3. Nel browser Web, fornire i dati di accesso e configurare le impostazioni di protezione della periferica.

Nota: se la periferica è un router o un punto di accesso senza fili protetto con Wireless Network Security, per configurare le impostazioni di protezione della periferica è necessario utilizzare Wireless Network Security.

Modifica delle proprietà di visualizzazione di una periferica

Quando si modificano le proprietà di visualizzazione di una periferica è possibile modificare il nome della periferica visualizzato e specificare se si tratta di un router senza fili.

Per modificare le proprietà di visualizzazione di una periferica:

1. Fare clic sull'icona di una periferica nella mappa della rete.
2. Fare clic su **Modificare le proprietà della periferica** nella sezione **Desidero**.
3. Per specificare il nome della periferica visualizzato, digitare un nome nella casella **Nome**.
4. Per specificare il tipo di periferica, fare clic su una delle seguenti opzioni:
   - **Router**
     Rappresenta un router domestico standard.
   - **Router wireless**
     Rappresenta un router domestico senza fili.
5. Fare clic su **OK**.

Risoluzione delle vulnerabilità della protezione

I computer gestiti con autorizzazioni con privilegi di amministratore possono monitorare lo stato della protezione McAfee di altri computer gestiti sulla rete e risolvere eventuali vulnerabilità segnalate in modalità remota. Ad esempio, se lo stato della protezione McAfee di un computer gestito indica che VirusScan è disattivato, un altro computer gestito con autorizzazioni con privilegi di amministratore può *risolvere* la vulnerabilità della protezione attivando VirusScan in modalità remota.

Quando si risolvono le vulnerabilità della protezione in modalità remota, Network Manager ripara automaticamente gran parte dei problemi segnalati. Tuttavia, alcune vulnerabilità della protezione potrebbero richiedere un intervento manuale sul computer locale. In tal caso, Network Manager corregge i problemi che è possibile riparare in modalità remota, quindi richiede all'utente di risolvere i restanti problemi effettuando l'accesso a SecurityCenter sul computer vulnerabile e attenendosi ai suggerimenti forniti. In alcuni casi, per correggere il problema si suggerisce di installare il software di protezione McAfee 2007 sul computer remoto o sui computer in rete.

Risoluzione delle vulnerabilità della protezione

È possibile utilizzare Network Manager per risolvere automaticamente gran parte delle vulnerabilità della protezione sui computer gestiti remoti. Ad esempio, se VirusScan è disattivato su un computer remoto, è possibile utilizzare Network Manager per attivarlo automaticamente.

Per risolvere le vulnerabilità della protezione:

1. Fare clic sull'icona di un elemento sulla mappa della rete.
2. Visualizzare lo stato della protezione dell'elemento nella sezione **Dettagli**.
3. Fare clic su **Risolvere vulnerabilità della protezione** nella sezione **Desidero**.
4. Dopo aver risolto i problemi di protezione, fare clic su **OK**.

Nota: benché Network Manager risolva automaticamente gran parte delle vulnerabilità della protezione, per l'esecuzione di alcune operazioni potrebbe essere necessario avviare SecurityCenter sul computer vulnerabile e attenersi ai suggerimenti forniti.

Installazione del software di protezione McAfee sui computer remoti

Se su uno o più computer in rete non è in esecuzione il software di protezione McAfee 2007, non è possibile monitorare in modalità remota il rispettivo stato della protezione. Se si desidera monitorare questi computer in modalità remota, è necessario installare il software di protezione McAfee su ciascuno di essi.

Per installare il software di protezione McAfee su un computer remoto:

1. Nel browser del computer remoto andare all'indirizzo http://download.mcafee.com/us/.
2. Seguire le istruzioni visualizzate per installare il software di protezione McAfee 2007 sul computer.

CAPITOLO 13

McAfee Wireless Network Security

Wireless Network Security fornisce protezione automatica, standard nel settore, contro furti di dati, accessi alla rete non autorizzati e utilizzo abusivo della connessione a banda larga ("freeloading") attraverso un'interfaccia intuitiva e di facile utilizzo mediante un solo clic. Wireless Network Security crittografa i dati personali e privati mentre vengono inviati sulla rete Wi-Fi e impedisce agli hacker di accedere alla rete senza fili.

Wireless Network Security blocca gli attacchi degli hacker alla rete senza fili:

- Impedendo connessioni non autorizzate alla rete Wi-Fi
- Impedendo l'acquisizione dei dati trasmessi su una rete Wi-Fi
- Rilevando i tentativi di connessione a una rete Wi-Fi

Wireless Network Security combina funzioni di facile uso quali il blocco immediato della rete e la possibilità di aggiungere rapidamente ad essa utenti legittimi, con funzioni di protezione affidabili quali la generazione automatica della chiave crittografata e la rotazione pianificata delle chiavi.

In questo capitolo

Funzioni

Wireless Home Network Security offre le seguenti funzioni.

Protezione sempre attiva

Rilevazione e protezione automatica di qualsiasi rete senza fili vulnerabile a cui si effettui una connessione.

Interfaccia intuitiva

Consente di proteggere la rete senza dover prendere decisioni difficili o conoscere termini tecnici complessi.

Crittografia avanzata automatica

Consente l'accesso alla rete solo a parenti e amici e protegge la trasmissione e la ricezione dei dati.

Soluzione solo software

Wireless Network Security funziona con router o punti di accesso senza fili standard e software di protezione. Non è necessario acquistare hardware addizionale.

Rotazione automatica delle chiavi

Persino gli hacker più determinati non possono acquisire le informazioni, poiché la chiave è in continua rotazione.

Aggiunta di utenti di rete:

consente di autorizzare facilmente parenti e amici ad accedere alla rete. Gli utenti possono essere aggiunti tramite rete senza fili, oppure trasferendo il software mediante un'unità USB.

Strumento di connessione intuitivo

Lo strumento di connessione senza fili è intuitivo e informativo, con dettagli sulla potenza del segnale e sullo stato della protezione.

Registrazione di eventi e avvisi

Segnalazioni e avvisi di facile comprensione offrono agli utenti più esperti ulteriori informazioni sulla rete senza fili.

Modalità sospensione

Consente di sospendere temporaneamente la rotazione delle chiavi in modo che particolari applicazioni possano funzionare senza interruzione.

Compatibilità con altri dispositivi

Wireless Network Security si aggiorna automaticamente con i moduli di router o punti di accesso senza fili più recenti delle marche più diffuse, tra cui: Linksys®, NETGEAR®, D-Link®, Belkin®, TRENDnet® e altri.

Avvio di Wireless Network Security

Dopo l'installazione, Wireless Network Security viene attivato automaticamente. Non è pertanto necessario avviarlo manualmente. Facoltativamente, tuttavia, è possibile attivare e disattivare manualmente la protezione senza fili.

Dopo aver installato Wireless Network Security, il computer tenta di stabilire una connessione con il router senza fili. Una volta stabilita la connessione, il computer programma la chiave di crittografia nel router senza fili. Se la password predefinita è stata cambiata, viene richiesta affinché Wireless Network Security possa configurare il router senza fili con la chiave di crittografia condivisa e una modalità di protezione avanzata. Anche il computer è configurato con la stessa chiave condivisa e la stessa modalità di crittografia, stabilendo una connessione senza fili protetta.

Avvio di Wireless Network Security

Wireless Network Security è attivato per impostazione predefinita. È tuttavia possibile attivare e disattivare manualmente la protezione senza fili.

L'attivazione di questa protezione salvaguarda la rete senza fili dalle intrusioni e dall'intercettazione dei dati. Tuttavia, se si è connessi a una rete senza fili esterna, la protezione del computer varia a seconda del livello di protezione della rete.

Per attivare manualmente la protezione senza fili:

1 Nel riquadro McAfee SecurityCenter, effettuare una delle seguenti operazioni:
   - Fare clic su **Rete e Internet**, quindi su **Configura**.
   - Fare clic su **Menu avanzato**, quindi su **Configura** nel riquadro **Home** e selezionare **Rete e Internet**.

2 Nel riquadro **Configurazione di Internet e rete**, fare clic su **Attiva** in **Wireless Protection**

Nota: se è installato un adattatore senza fili compatibile, Wireless Network Security viene attivato automaticamente.

Arresto di Wireless Network Security

Wireless Network Security è attivato per impostazione predefinita. È tuttavia possibile attivare e disattivare manualmente la protezione senza fili.

Se si disattiva la protezione senza fili, la rete rimane esposta a intrusioni e all'intercettazione dei dati.

Per disattivare la protezione senza fili:

1. Nel riquadro McAfee SecurityCenter, effettuare una delle seguenti operazioni:
   - Fare clic su **Rete e Internet**, quindi su **Configura**.
   - Fare clic su **Menu avanzato**, quindi su **Configura** nel riquadro **Home** e selezionare **Rete e Internet**.
2. Nel riquadro **Configurazione di Internet e rete**, fare clic su **Disattiva** in **Wireless Protection**.

CAPITOLO 14

Protezione delle reti senza fili

Wireless Network Security protegge la rete implementando la crittografia senza fili tramite WEP, WPA o WPA2, in base al dispositivo utilizzato. Programma automaticamente i client e i router senza fili con le credenziali della chiave di crittografia valide affinché il router senza fili autorizzi i computer a collegarsi. Le reti senza fili protette con la crittografia bloccano l'accesso alla rete senza fili da parte di utenti non autorizzati e proteggono i dati inviati su una rete senza fili. Wireless Network Security ottiene questi risultati:

- Creando e distribuendo una chiave di crittografia lunga, complessa, casuale e condivisa
- Ruotando la chiave di crittografia in maniera programmata
- Configurando ogni dispositivo senza fili con chiavi di crittografia

In questo capitolo

Impostazione di reti senza fili protette

Quando Wireless Network Security è installato, chiede automaticamente all'utente di proteggere la rete senza fili non protetta alla quale è collegato o di diventare membro di una rete senza fili protetta in precedenza.

Se non si è connessi a una rete senza fili, Wireless Network Security esegue una scansione per individuare una rete protetta da McAfee con una forte potenza del segnale e chiede all'utente di diventarne membro. Se non è disponibile nessuna rete protetta, Wireless Network Security esegue la scansione per individuare le reti non protette con segnali potenti e quando ne individua una, chiede all'utente di proteggerla.

Se una rete senza fili non è stata protetta da McAfee Wireless Network Security, McAfee la considera "non protetta" anche se vengono utilizzati meccanismi di protezione senza fili quali WEP e WPA.

Se una rete senza fili non è protetta da Wireless Network Security, McAfee la considera non protetta anche se vengono utilizzati meccanismi di protezione senza fili quali WEP e WPA.

Informazioni sui tipi di accesso

Qualsiasi computer senza fili in cui è installato Wireless Network Security può creare una rete senza fili protetta. Al primo computer che protegge un router e crea una rete senza fili protetta viene automaticamente concesso l'accesso con privilegi di amministratore su quella rete. Ai computer aggiunti in seguito può essere concesso l'accesso con privilegi di amministratore, completo o Guest da parte di un utente esistente che dispone di accesso con privilegi di amministratore.

I computer con tipi di accesso con privilegi di amministratore e completo possono svolgere le seguenti attività:

- Proteggere e rimuovere un router o un punto di accesso
- Ruotare le chiavi di protezione
- Cambiare le impostazioni di protezione della rete
- Ripristinare le reti
- Concedere ai computer l'accesso alla rete
- Revocare l'accesso alla rete senza fili protetta
- Cambiare il livello di amministrazione di un computer

I computer con tipi di accesso Guest possono svolgere le seguenti attività nella rete:

- Connettersi a una rete
- Diventare membri di una rete
- Modificare le impostazioni specifiche per il computer guest

Nota: i computer possono disporre dell'accesso con privilegi di amministratore su una rete senza fili ma solo dell'accesso Guest o completo su un'altra. Un computer con accesso Guest o completo su una rete può creare una nuova rete.

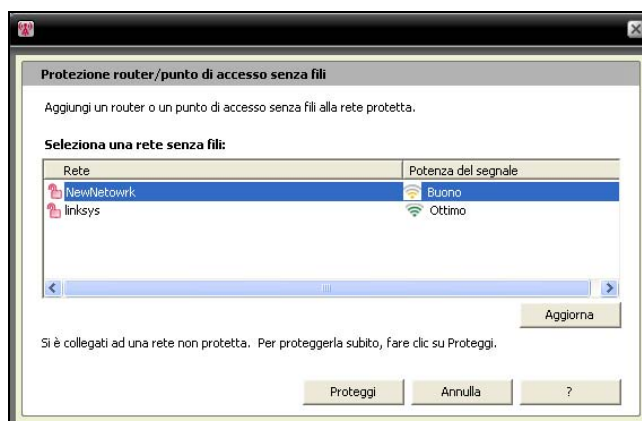
Argomenti correlati

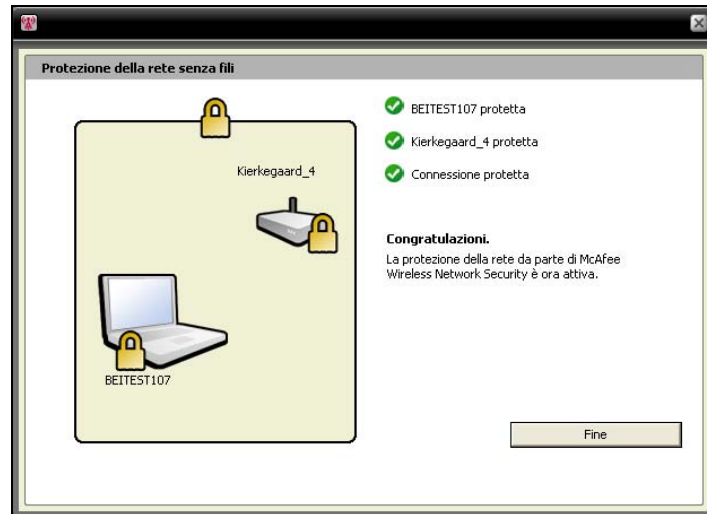
- **Aggiunta a una rete senza fili protetta** (pagina 80)
- **Concessione dell'accesso con privilegi di amministratore ai computer** (pagina 84)
- **Revoca dell'accesso alla rete** (pagina 104)

Creazione di reti senza fili protette

Per creare una rete senza fili protetta, è prima necessario aggiungere il router o il punto di accesso senza fili della rete senza fili.

Per aggiungere un router o un punto di accesso senza fili:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza strumenti**.
3. Nel riquadro Strumenti di protezione, in **Protezione router/punto di accesso senza fili**, fare clic su **Proteggi**.
4. Nel riquadro Protezione router/punto di accesso senza fili selezionare una rete senza fili da proteggere, quindi fare clic su **Proteggi**.

Quando Wireless Network Security tenta di proteggere il computer, il router e la connessione di rete, viene visualizzato il riquadro Protezione della rete senza fili.

La protezione corretta di tutti questi componenti comporta la protezione totale della rete senza fili.

5 Fare clic su **Fine**.

Nota: dopo aver protetto una rete, la finestra di dialogo Operazioni successive ricorda di installare Wireless Network Security in tutti i computer senza fili per consentire che diventino membri della rete.

Se in precedenza era stata configurata manualmente una chiave già condivisa per il proprio router o punto di accesso ma non si era connessi quando si è tentato di proteggere il router o il punto di accesso, è necessario immettere anche la chiave nella casella Chiave WEP, quindi fare clic su Connetti. Se in precedenza il nome utente amministrativo o la password erano stati modificati, viene chiesto di immettere queste informazioni per proteggere un router o un punto di accesso.

Argomenti correlati

- **Protezione di altri dispositivi senza fili** (pagina 86)
- **Aggiunta di computer alla rete senza fili protetta** (pagina 88)

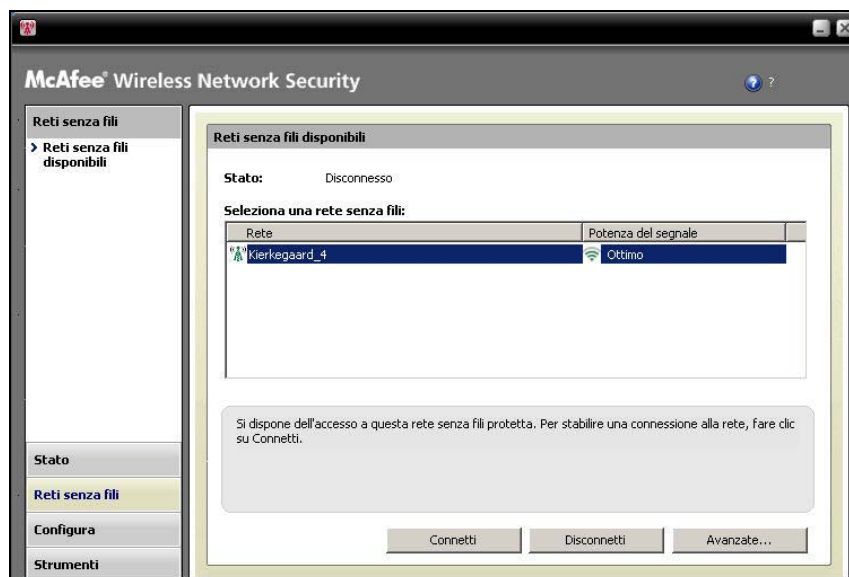
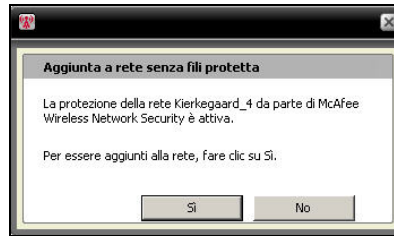
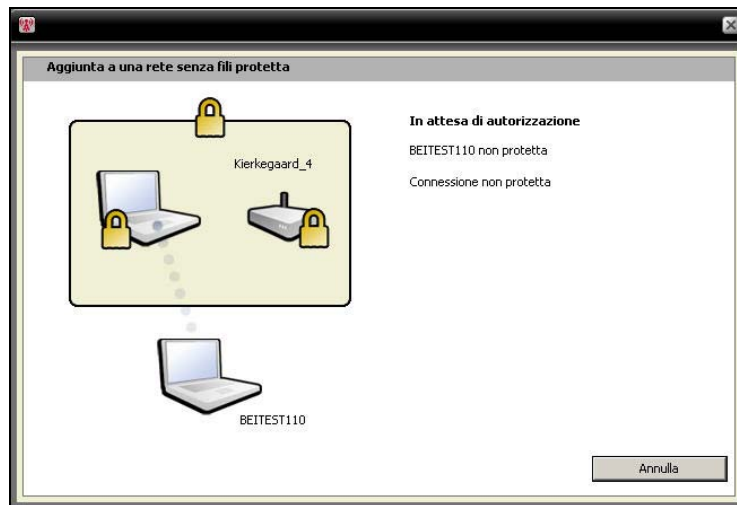
Diventare membri di una rete senza fili protetta

Una rete protetta impedisce agli hacker di intercettare i dati che vengono trasmessi sulla rete e di collegarsi alla rete dell'utente. Prima che un computer autorizzato possa accedere a una rete senza fili protetta, è necessario che ne diventi membro.

Quando un computer chiede di diventare membro di una rete gestita, viene inviato un messaggio agli altri computer in rete che dispongono di accesso con privilegi di amministratore. L'utente amministratore di questo computer sarà responsabile della scelta del tipo di accesso: Guest, completo o con privilegi di amministratore.

Prima di poter diventare membro di una rete protetta, è necessario installare Wireless Network Security e quindi collegarsi alla rete senza fili protetta. Un utente di rete esistente con accesso con privilegi di amministratore sulla rete senza fili protetta deve consentire al nuovo utente di diventarne membro. Dopo essere diventati membri della rete non è necessario chiedere di essere nuovamente aggiunti a ogni riconnessione. Sia chi concede l'autorizzazione sia l'utente che ha ricevuto tale autorizzazione devono disporre di una connessione senza fili attiva. Chi concede l'accesso deve essere un computer con diritti di amministratore connesso alla rete.

Per diventare membro di una rete senza fili protetta:

1. Nel computer non protetto fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza reti senza fili**.
3. Nel riquadro Reti senza fili disponibili selezionare una rete, quindi fare clic su **Connetti**.

4 Nella finestra di dialogo Aggiunta a rete senza fili protetta fare clic su **Sì** per diventare membro della rete.

Quando Wireless Network Security tenta di richiedere l'autorizzazione a diventare membro della rete, viene visualizzato il riquadro Aggiunta a una rete senza fili protetta nel computer che tenta di aggiungersi alla rete.

5 Il riquadro Aggiunta di un membro alla rete viene visualizzato nel computer dell'amministratore dal quale può essere concesso l'accesso Guest, completo o con privilegi di amministratore.

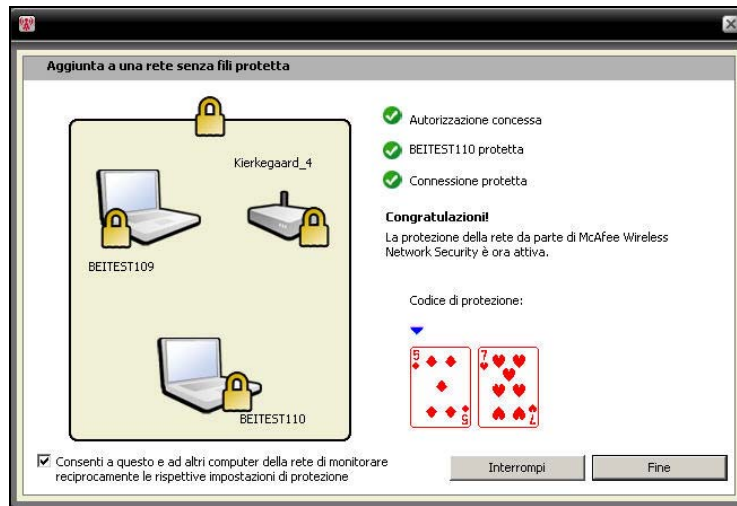
Nella finestra di dialogo Aggiunta di un membro alla rete selezionare una delle seguenti opzioni:

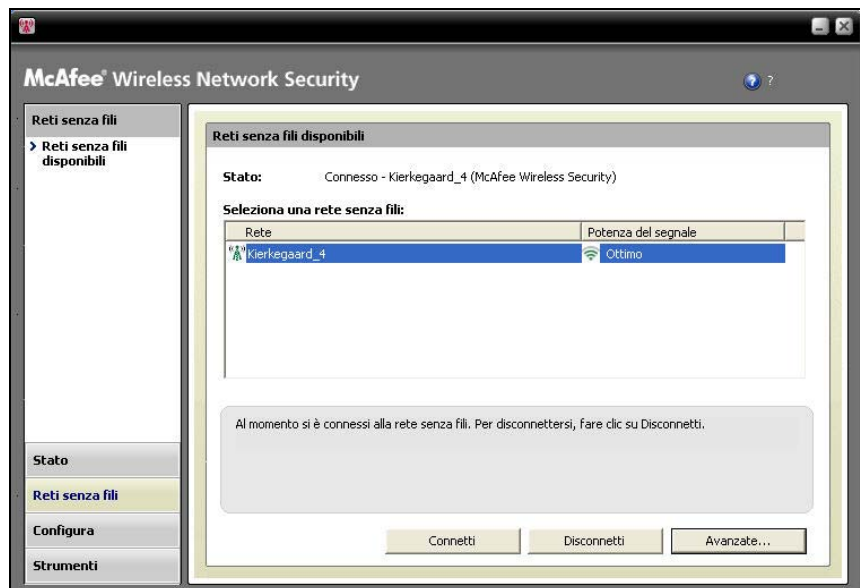
Concedi accesso Guest	Consente al computer di inviare file ad altri computer nella rete senza fili ma non di condividere file con McAfee EasyNetwork.
Concedi accesso completo a tutte le applicazioni della rete gestita	Consente al computer di inviare e condividere file con McAfee EasyNetwork.
Concedi accesso con privilegi di amministratore a tutte le applicazioni della rete gestita	Consente al computer di inviare e condividere file con McAfee EasyNetwork, concedere l'accesso ad altri computer e regolare i livelli di accesso di altri computer nella rete senza fili.

6 Fare clic su **Consenti accesso**.

7 Controllare che le carte visualizzate nel riquadro Concessione accesso alla rete in corso corrispondano a quelle visualizzate nel computer che tenta di aggiungersi alla rete senza fili. Se le carte corrispondono fare clic su **Concedi accesso**.

Se i computer non visualizzano le stesse carte da gioco, si è verificata una potenziale violazione della protezione. La concessione a questo computer dell'accesso alla rete potrebbe esporre a rischi il proprio computer. Per impedire al computer di accedere alla rete senza fili, fare clic su **Rifiuta accesso**.

8 Nel riquadro Concessione accesso alla rete in corso viene visualizzata la conferma che il nuovo computer è protetto da Wireless Network Security. Per monitorare le impostazioni di protezione di, e per essere monitorati da, altri computer, selezionare **Consenti a questo e ad altri computer della rete di monitorare reciprocamente le rispettive impostazioni di protezione.**

9 Fare clic su **Fine**.

10 Nel riquadro Reti senza fili disponibili è indicato che si è connessi alla rete senza fili protetta.

Argomenti correlati

- **Aggiunta di computer alla rete senza fili protetta** (pagina 88)

Connessione a reti senza fili protette

Se si è già membri di una rete senza fili protetta ma in seguito ci si è disconnessi e l'accesso non è stato revocato, è possibile riconnettersi in qualsiasi momento senza dover chiedere di essere nuovamente aggiunti.

Per stabilire una connessione a una rete senza fili protetta:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza reti senza fili**.
3. Nel riquadro Reti senza fili disponibili selezionare una rete, quindi fare clic su **Connetti**.

Concessione dell'accesso con privilegi di amministratore ai computer

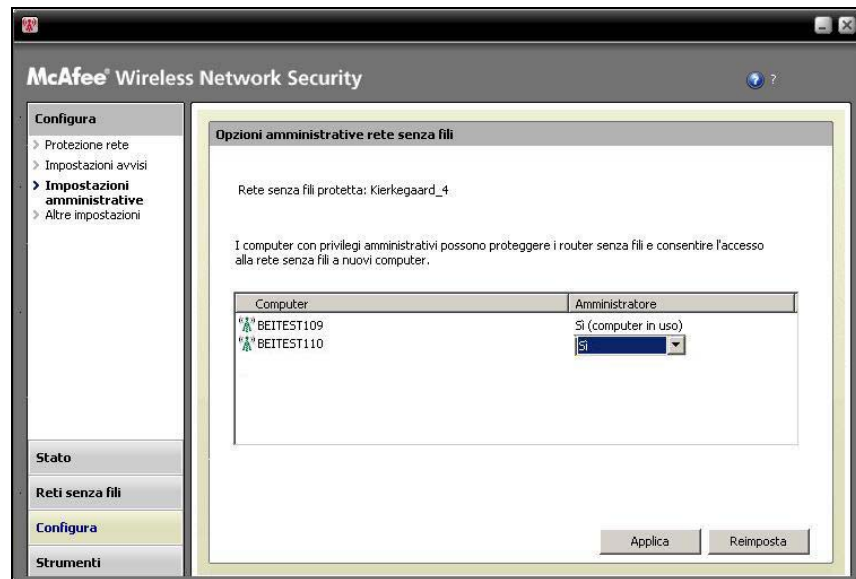
I computer con privilegi di amministratore possono proteggere i router senza fili, cambiare le modalità di protezione e consentire a nuovi computer l'accesso alla rete senza fili protetta.

Per configurare l'accesso con privilegi di amministratore:

1 Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.

2 Selezionare **Visualizza configurazione**.

3 Nel riquadro Configura, selezionare **Impostazioni amministrative**.

4 Nel riquadro Opzioni amministrative rete senza fili selezionare **Sì** o **No** per consentire o non consentire l'accesso con privilegi di amministratore.

5 Fare clic su **Applica**.

Argomenti correlati

- **Informazioni sui tipi di accesso** (pagina 77)
- **Revoca dell'accesso alla rete** (pagina 104)

Protezione di altri dispositivi senza fili

Wireless Network Security consente di aggiungere alla rete una o più stampanti, server di stampa o console per giochi senza fili.

Per aggiungere una stampante, un server di stampa o una console per giochi senza fili:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza strumenti**.
3. Nel riquadro Strumenti di protezione, in **Protezione dispositivi non di accesso**, fare clic su **Proteggi**.
4. Nel riquadro Protezione dispositivo senza fili selezionare un dispositivo senza fili, quindi fare clic su **Proteggi**.
5. L'avviso Dispositivo non di accesso protetto conferma che il dispositivo è stato aggiunto alla rete.

Connessione a reti con trasmissione SSID disattivata

È possibile connettersi a reti senza fili la cui trasmissione SSID sia disattivata. Quando i router hanno la trasmissione SSID disattivata, non vengono visualizzati nel riquadro Reti senza fili disponibili.

McAfee consiglia di non proteggere con Wireless Network Security router senza fili che hanno la trasmissione SSID disattivata.

Per connettersi a una rete senza fili con la trasmissione SSID disattivata:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza reti senza fili**.
3. Nel riquadro Reti senza fili disponibili, fare clic su **Avanzate**.
4. Nel riquadro Reti senza fili, fare clic su **Aggiungi**.
5. Nel riquadro Aggiunta rete senza fili specificare le seguenti impostazioni, quindi fare clic su **OK**:

Impostazione	Descrizione
Rete	Nome della rete. Se si sta modificando una rete, non è possibile cambiarne il nome.
Impostazioni protezione	Protezione della rete non protetta. Se l'adattatore senza fili non supporta la modalità selezionata, la connessione non è possibile. Le modalità di protezione comprendono: Disattivata, WEP aperta, WEP condivisa, WEP automatica, WPA-PSK, WPA2-PSK.
Modalità crittografia	Crittografia associata alla modalità di protezione selezionata. Le modalità di crittografia comprendono: WEP, TKIP, AES e TKIP+AES.

Nota: McAfee consiglia di non proteggere con Wireless Network Security router senza fili che hanno la trasmissione SSID disattivata. Se è necessario utilizzare questa funzione, farlo solo se la trasmissione SSID è disattivata.

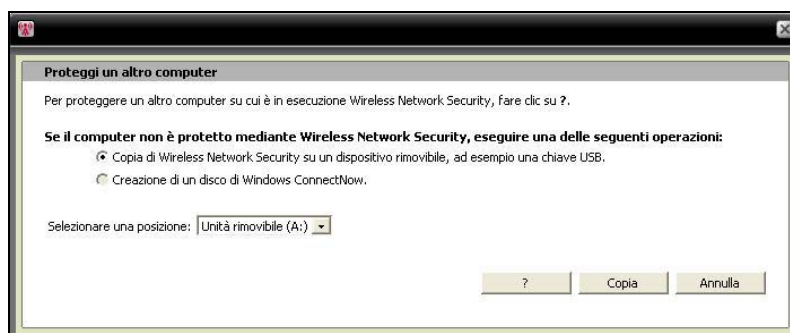
Aggiunta di computer alla rete senza fili protetta

È possibile aggiungere computer alla rete senza fili protetta utilizzando un dispositivo rimovibile, ad esempio un'unità flash USB, un CD scrivibile o la tecnologia Windows Connect Now.

Aggiunta di computer tramite un dispositivo rimovibile

Wireless Network Security consente di aggiungere altri computer alla rete senza fili protetta che non eseguono Wireless Network Security, utilizzando un'unità flash USB o un CD scrivibile.

Per aggiungere un computer:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza strumenti**.
3. Nel riquadro Strumenti di protezione, in **Protezione computer**, fare clic su **Proteggi**.
4. Nel riquadro Proteggi un altro computer selezionare **Copia di Wireless Network Security su un dispositivo rimovibile, ad esempio una chiave USB**.

5 Selezionare il percorso dell'unità CD o dell'unità flash USB in cui copiare Wireless Network Security.

6 Fare clic su **Copia**.

7 Dopo aver copiato tutti i file nel CD o nell'unità flash USB, inserire il dispositivo rimovibile nel computer che si desidera proteggere. Se il programma non si avvia automaticamente, scorrere il contenuto del dispositivo rimovibile da Esplora risorse di Windows, quindi fare clic su **Install.exe**.

8 Seguire le istruzioni riportate sullo schermo.

Nota: è anche possibile aggiungere un computer alla rete senza fili protetta utilizzando la tecnologia Windows Connect Now.

Argomenti correlati

- **Aggiunta di computer utilizzando la tecnologia Windows Connect Now** (pagina 90)

Aggiunta di computer utilizzando la tecnologia Windows Connect Now

Wireless Network Security consente di aggiungere altri computer alla rete che non eseguono Wireless Network Security, utilizzando la tecnologia Windows Connect Now.

Per aggiungere un computer utilizzando la tecnologia Windows Connect Now:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza strumenti**.
3. Nel riquadro Strumenti di protezione, in **Protezione computer**, fare clic su **Proteggi**.
4. Nel riquadro Proteggi un altro computer selezionare **Creazione di un disco di Windows ConnectNow.**
5. Selezionare un percorso in cui copiare le informazioni su Windows Connect Now.
6. Fare clic su **Copia**.
7. Inserire il disco Windows Connect Now nel computer che si desidera proteggere
8. Se il disco non si avvia automaticamente, eseguire una delle seguenti operazioni:
   - Installare la tecnologia Windows Connect Now: fare clic su **Start** dalla barra delle applicazioni di Windows, quindi su Pannello di controllo. Se si utilizza la visualizzazione Categoria del Pannello di controllo, fare clic su **Rete e connessioni Internet**, quindi fare clic su **Installazione guidata rete senza fili**. Se si utilizza la visualizzazione classica del Pannello di controllo, fare clic su **Installazione guidata rete senza fili**. Seguire le istruzioni riportate sullo schermo.
   - Aprire `setupSNK.exe` nel disco Windows Connect e copiare e incollare la chiave nel client di selezione della rete senza fili.

Nota: sospendere la rotazione delle chiavi se si utilizza la tecnologia Windows Connect per connettersi alla rete senza fili; in caso contrario la connessione di rete non riuscirà. La connessione non riesce perché la rotazione delle chiavi crea una nuova chiave diversa da quella utilizzata dalla tecnologia Windows Connect Now.

È anche possibile aggiungere computer alla rete senza fili protetta utilizzando un dispositivo rimovibile, ad esempio un'unità flash USB o un CD scrivibile.

Argomenti correlati

- **Aggiunta di computer tramite un dispositivo rimovibile** (pagina 88)

CAPITOLO 15

Amministrazione delle reti senza fili

Wireless Network Security offre una serie completa di strumenti di amministrazione per agevolare la gestione e la manutenzione della rete senza fili.

In questo capitolo

Gestione delle reti senza fili

Quando si è connessi a una rete senza fili protetta, le informazioni inviate e ricevute vengono crittografate. Gli hacker non possono decrittografare i dati che vengono trasmessi sulla rete protetta e non possono connettersi alla rete. Wireless Network Security offre numerosi strumenti che agevolano la gestione della rete per impedire ulteriori intrusioni.

Informazioni sulle icone di Wireless Network Security

Wireless Network Security visualizza icone che rappresentano vari tipi di connessione di rete e di potenza del segnale.

Icone della connessione di rete

Nella tabella seguente vengono descritte le icone utilizzate comunemente da Wireless Network Security nei riquadri Stato rete senza fili e gli strumenti di protezione disponibili nei riquadri Reti senza fili disponibili. Le icone rappresentano vari stati di connessione e di protezione della rete.

Icona	Riquadri dello stato	Riquadri di protezione
	Il computer è connesso alla rete senza fili protetta selezionata.	Il dispositivo è protetto da Wireless Network Security.
	Il computer può accedere alla rete senza fili protetta ma attualmente non è connesso.	Il dispositivo utilizza la protezione WEP o WPA.
	Il computer è un ex membro della rete senza fili protetta ma l'accesso è stato revocato quando il computer è stato disconnesso dalla rete.	Nel dispositivo, Wireless Network Security è disattivato.

Icone della potenza del segnale

Nella tabella seguente vengono descritte le icone utilizzate comunemente da Wireless Network Security per rappresentare le varie potenze del segnale di rete.

Icona	Descrizione
	Potenza del segnale eccellente
	Potenza del segnale ottima
	Potenza del segnale buona
	Potenza del segnale bassa

Argomenti correlati

- **Visualizzazione della potenza del segnale della rete** (pagina 130)
- **Visualizzazione dei computer attualmente protetti** (pagina 138)
- **Visualizzazione della modalità di protezione della rete** (pagina 127)

Elenco delle reti preferite

Wireless Network Security consente di specificare le reti senza fili preferite. In tal modo è possibile specificare l'ordine delle reti alle quali il computer si connette automaticamente. Wireless Network Security tenta di connettersi alla prima rete che compare nell'elenco.

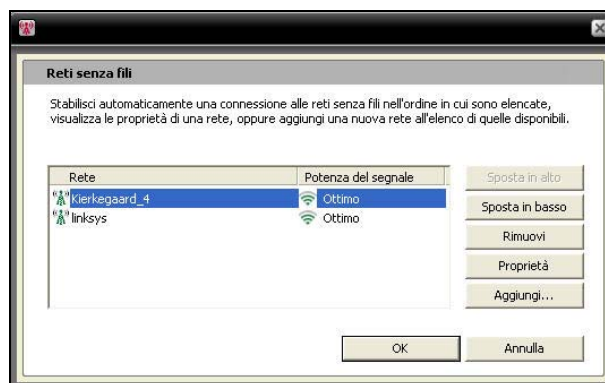
Queste funzioni sono utili quando, ad esempio, si desidera connettersi automaticamente alla rete senza fili dell'amico quando ci si trova nella sua area. È possibile innalzare di livello un'altra rete facendola comparire in cima all'elenco.

Per elencare le reti preferite:

1 Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.

2 Selezionare **Visualizza reti senza fili**.

3 Nel riquadro Reti senza fili disponibili, fare clic su **Avanzate**.

4 Selezionare la rete di cui si desidera modificare l'ordine, quindi fare clic su **Sposta in alto** o **Sposta in basso**.

5 Fare clic su **OK**.

Argomenti correlati

- **Rimozione delle reti senza fili preferite** (pagina 97)

Rimozione delle reti senza fili preferite

È possibile utilizzare Wireless Network Security per rimuovere le reti preferite.

Ciò è utile quando, ad esempio, si desidera rimuovere una rete obsoleta dall'elenco.

Per rimuovere le reti preferite:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza reti senza fili**.
3. Nel riquadro Reti senza fili disponibili, fare clic su **Avanzate**.
4. Nel riquadro delle reti senza fili selezionare una rete, quindi fare clic su **Rimuovi**.
5. Fare clic su **OK**.

Argomenti correlati

- **Elenco delle reti preferite** (pagina 96)

Ridenominazione di reti senza fili protette

È possibile utilizzare Wireless Network Security per rinominare la rete senza fili protetta esistente.

La ridenominazione della rete può essere utile se il suo nome è simile o identico a uno utilizzato dal vicino o se si desidera creare un nome univoco per poterla distinguere più facilmente.

I computer connessi alla rete senza fili protetta potrebbero doversi riconnettere manualmente e ricevono una notifica nel caso in cui il nome cambi.

Dopo aver rinominato la rete, il nuovo nome viene visualizzato nel riquadro Protezione router/punto di accesso senza fili.

Per modificare il nome della rete senza fili protetta:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza configurazione**.
3. Nel riquadro Protezione rete digitare il nuovo nome nella casella **Nome rete senza fili protetta**.
4. Fare clic su **Applica**.

   Quando Wireless Network Security cambia il nome della rete senza fili protetta, viene visualizzata la finestra di dialogo Aggiornamento delle impostazioni di protezione della rete in corso... Il nome del computer cambia in meno di un minuto, in base alle impostazioni del computer e alla potenza del segnale.

Nota: come misura di protezione, McAfee consiglia di rinominare l'SSID predefinito del router o del punto di accesso. Sebbene Wireless Network Security supporti SSID predefiniti quali "linksys" o "belkin54g" o "NETGEAR", la ridenominazione degli SSID protegge da minacce mascherate al punto di accesso.

Configurazione delle impostazioni di avviso

Wireless Network Security consente di configurare le impostazioni di avviso quando si verificano determinati eventi, ad esempio quando un nuovo computer si connette alla rete dell'utente.

Per configurare il comportamento di avviso:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza configurazione**.
3. Fare clic su **Impostazioni avviso**.
4. Selezionare o deselezionare uno o più degli eventi seguenti, quindi fare clic su **Applica**:

Impostazione dell'avviso	Descrizione
Quando si verifica la rotazione delle chiavi di protezione per la rete senza fili protetta.	Visualizza l'avviso Chiave di protezione rotata dopo che la chiave di protezione è stata ruotata manualmente o automaticamente. La rotazione delle chiavi protegge la rete dagli hacker che tentano di intercettare i dati dell'utente o di connettersi alla sua rete.
Quando un altro computer protetto si collega alla rete o interrompe la connessione.	Visualizza l'avviso Computer connesso o Computer non connesso dopo che un computer si connette o disconnette dalla rete senza fili protetta. I dati presenti nei computer connessi sono ora protetti da intrusioni e intercettazioni.
Quando a un altro computer viene concesso l'accesso alla rete senza fili protetta.	Visualizza l'avviso Accesso alla rete concesso al computer dopo che il computer di un amministratore concede a un altro computer di aggiungersi alla rete senza fili protetta. La concessione a un computer dell'accesso alla rete protetta lo protegge dai tentativi degli hacker di intercettare i dati dell'utente.
Quando a rotazione delle chiavi per una rete senza fili protetta viene sospesa o ripresa.	Visualizza l'avviso Rotazione delle chiavi sospesa o Rotazione delle chiavi ripresa dopo che la rotazione delle chiavi è stata sospesa o ripresa manualmente. La rotazione delle chiavi protegge la rete dagli hacker che tentano di intercettare i dati dell'utente o di connettersi alla sua rete.
Quando viene revocato l'accesso di tutti i computer non connessi.	Visualizza l'avviso Accesso revocato dopo la revoca dell'accesso per i computer non connessi alla rete che dovranno essere nuovamente aggiunti alla rete.
Quando un router viene aggiunto alla rete senza fili protetta o rimosso da essa.	Visualizza l'avviso Router/punto di accesso senza fili aggiunto alla rete o Router/punto di accesso senza fili non protetto dopo che il router o il punto di accesso senza fili è stato aggiunto o rimosso dalla rete senza fili protetta.
Quando i dati di accesso per un router senza fili protetto vengono modificati.	Visualizza l'avviso Dati di accesso a router/punto di accesso modificati dopo che l'amministratore di Wireless Network Security cambia il nome utente o la password per un router o un punto di accesso.

Quando il nome o le impostazioni di protezione della rete senza fili protetta vengono modificati.	Visualizza l'avviso Impostazioni di rete modificate o rete ridenominata dopo la ridenominazione della rete senza fili protetta o la rettifica della sua impostazione di protezione.
Quando vengono riparate le impostazioni della rete senza fili protetta.	Visualizza l'avviso Rete riparata dopo la risoluzione delle impostazioni di protezione nei router o nei punti di accesso senza fili della rete.

Nota: per scegliere o deselezionare tutte le impostazioni di avviso, fare clic rispettivamente su **Seleziona tutto** o **Deseleziona tutto**. Per ripristinare le impostazioni di avviso di Wireless Network Security, fare clic su **Ripristina impostazioni predefinite**.

Argomenti correlati

- **Rotazione automatica delle chiavi** (pagina 114)
- **Aggiunta a una rete senza fili protetta** (pagina 80)
- **Connessione a reti senza fili protette** (pagina 84)
- **Disconnessione da reti senza fili protette** (pagina 103)
- **Sospensione della rotazione automatica delle chiavi** (pagina 117)
- **Revoca dell'accesso alla rete** (pagina 104)
- **Rimozione di router o punti di accesso senza fili** (pagina 102)
- **Modifica delle credenziali per dispositivi senza fili** (pagina 111)
- **Ridenominazione di reti senza fili protette** (pagina 97)
- **Ripristino delle impostazioni di protezione della rete** (pagina 112)

Visualizzazione delle notifiche di connessione

È possibile configurare Wireless Network Security per ricevere una notifica quando il proprio computer si connette a una rete senza fili.

Per visualizzare la notifica quando ci si connette a una rete senza fili:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza configurazione**.
3. Fare clic su **Altre impostazioni**.
4. Selezionare **Visualizza un messaggio di notifica quando si è connessi a una rete senza fili**.
5. Fare clic su **Applica**.

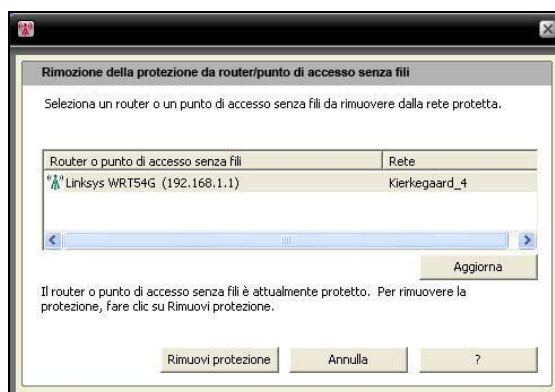
Argomenti correlati

- **Connessione a reti senza fili protette** (pagina 84)

Rimozione di router o punti di accesso senza fili

Wireless Network Security consente di rimuovere uno o più router o punti di accesso dalla rete protetta.

Per rimuovere un router o un punto di accesso senza fili:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza strumenti**.
3. Nel riquadro Strumenti di protezione, in **Rimozione della protezione da un dispositivo**, fare clic su **Rimuovi protezione**.
4. Nel riquadro Rimozione della protezione da router/punto di accesso senza fili selezionare un router o un punto di accesso da rimuovere dalla rete protetta, quindi fare clic su **Rimuovi protezione**.

5. Fare clic su **OK** nella finestra di dialogo Router/punto di accesso senza fili non protetto per confermare che il router o il punto di accesso senza fili è stato rimosso dalla rete.

Argomenti correlati

- **Creazione di reti senza fili protette** (pagina 78)

Disconnessione da reti senza fili protette

Wireless Network Security consente di disconnettere il computer dalla rete.

Questa operazione è utile quando, ad esempio, il computer si è connesso a una rete utilizzando un nome identico a quello della rete dell'utente. È possibile disconnettersi dalla rete, quindi riconnettersi alla propria.

Questa funzione è utile anche quando ci si connette accidentalmente alla rete sbagliata o a causa della potenza del segnale di un altro punto di accesso o a causa di un'interferenza radio.

Per disconnettersi da una rete senza fili protetta:

1 Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.

2 Selezionare **Visualizza reti senza fili**.

3 Nel riquadro Reti senza fili disponibili selezionare una rete, quindi fare clic su **Disconnetti**.

Argomenti correlati

- **Revoca dell'accesso alla rete** (pagina 104)
- **Abbandono di reti senza fili protette** (pagina 105)

Revoca dell'accesso alla rete

Wireless Network Security consente di revocare l'accesso per i computer che non sono connessi alla rete. Viene stabilito un nuovo programma di rotazione delle chiavi di protezione: i computer non connessi perderanno l'accesso alla rete senza fili protetta ma potranno riottenerlo venendo nuovamente aggiunti ad essa. L'accesso per i computer connessi viene mantenuto.

Ad esempio, è possibile revocare l'accesso del computer di un visitatore con Wireless Network Security dopo che si è disconnesso. Inoltre, un adulto può revocare l'accesso di un computer utilizzato da un bambino come forma di controllo genitori sull'accesso a Internet. Anche l'accesso per un computer concesso accidentalmente può essere revocato.

Per revocare l'accesso per tutti i computer disconnessi dalla rete protetta:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza strumenti**.
3. Nel riquadro Strumenti, fare clic su Strumenti di manutenzione.
4. Nel riquadro Strumenti di manutenzione, in **Revoca accesso**, fare clic su **Revoca**.
5. Nel riquadro Revoca accesso fare clic su **Revoca**.
6. Fare clic su **OK** nella finestra di dialogo Wireless Network Security.

Argomenti correlati

- **Disconnessione da reti senza fili protette** (pagina 103)
- **Abbandono di reti senza fili protette** (pagina 105)

Abbandono di reti senza fili protette

È possibile utilizzare Wireless Network Security per annullare i diritti di accesso a una rete protetta.

Per abbandonare una rete:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza configurazione**.
3. Nel riquadro Configura, fare clic su **Altre impostazioni**.
4. Nel riquadro Altre impostazioni, in Accesso alla rete protetta, selezionare la rete che si desidera abbandonare, quindi fare clic su **Abbandona rete**.
5. Nel riquadro Disconnetti dalla rete fare clic su **Sì** per abbandonare la rete.

Nota: quando si abbandona una rete, un altro utente può concedere l'accesso alla rete protetta prima di essere nuovamente aggiunti ad essa.

Argomenti correlati

- **Disconnessione da reti senza fili protette** (pagina 103)
- **Revoca dell'accesso alla rete** (pagina 104)

CAPITOLO 16

Gestione della protezione di rete senza fili

Wireless Network Security offre una serie completa di strumenti per agevolare la gestione delle funzioni di protezione della rete senza fili.

In questo capitolo

Configurazione delle impostazioni di protezione

Dopo essersi connessi a una rete senza fili protetta, Wireless Network Security protegge automaticamente la rete dell'utente; tuttavia è possibile configurare ulteriori impostazioni di protezione in qualsiasi momento.

Configurazione delle modalità di protezione

È possibile specificare la modalità di protezione della rete senza fili protetta. Le modalità di protezione definiscono la crittografia tra il computer e il router o il punto di accesso.

Quando si protegge la rete, WEP viene configurato automaticamente. Tuttavia, McAfee consiglia di cambiare la modalità di protezione scegliendo WPA2 o WPA-PSK AES. Wireless Network Security utilizza inizialmente WEP perché questa modalità è supportata da tutti i router e gli adattatori di rete senza fili. La maggior parte dei nuovi router e adattatori di rete senza fili, tuttavia, opera in modalità WPA, che è più sicura.

Per cambiare la modalità di protezione per una rete senza fili protetta:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza configurazione**.
3. Nel riquadro Protezione rete selezionare il tipo di protezione che si desidera implementare dalla casella **Modalità di protezione**, quindi fare clic su **Applica**.

Nella tabella seguente vengono descritte le modalità di protezione disponibili:

Classe di protezione	Modalità	Descrizione
Più debole	WEP	Wired Equivalent Privacy (WEP) fa parte dello standard di rete senza fili IEEE 802.11 a protezione delle reti senza fili IEEE 802.11. WEP fornisce un livello di protezione in grado di evitare intrusioni non sofisticate ma in genere non è sicuro quanto la crittografia WPA-PSK. Sebbene Wireless Network Security offra una chiave complessa (lunga e difficile da indovinare), McAfee consiglia di utilizzare una modalità di protezione WPA.
Media	WPA-PSK TKIP	Wi-Fi Protected Access (WPA) è una versione precedente dello standard di protezione 802.11i. TKIP è progettato per WPA per migliorare WEP. TKIP fornisce integrità del messaggio, meccanismo di reimpostazione delle chiavi e combinazione di chiavi per pacchetto
Elevata	WPA-PSK AES	Questa modalità di protezione combina le modalità WPA e AES. Advanced Encryption Standard (AES) è una crittografia a blocchi adottata come standard di crittografia da parte del governo statunitense.
Molto elevata	WPA2-PSK AES	Questa modalità di protezione combina le modalità WPA2 e AES. WPA2 è l'aggiornamento successivo alla ratifica dello standard di protezione 802.11i. WPA2 utilizza Counter Mode CBC MAC Protocol (CCMP), una soluzione più sicura e scalabile rispetto a TKIP. Questa è la modalità di protezione più robusta a disposizione a livello consumer.
Massima	WPA2-PSK TKIP+AES	Questa modalità di protezione combina le modalità WPA2 e AES e WPA-PSK TKIP. Consente una maggiore flessibilità per la connessione degli adattatori senza fili sia vecchi che nuovi.

Nota: dopo aver modificato la modalità di protezione, potrebbe venire richiesto di eseguire la riconnessione manualmente.

Argomenti correlati

- **Ripristino delle impostazioni di protezione della rete** (pagina 112)
- **Visualizzazione della modalità di protezione della rete** (pagina 127)

Configurazione delle impostazioni di protezione della rete

È possibile modificare le proprietà delle reti protette da Wireless Network Security. Ciò è utile quando, ad esempio, si desidera aggiornare la protezione da WEP a WPA.

McAfee consiglia di modificare le impostazioni di protezione della rete se un avviso suggerisce di farlo.

Per configurare le proprietà di una rete non protetta:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza reti senza fili**.
3. Nel riquadro Reti senza fili disponibili, fare clic su **Avanzate**.
4. Nel riquadro Reti senza fili, fare clic su **Proprietà**.
5. Nel riquadro Proprietà rete senza fili modificare le seguenti impostazioni, quindi fare clic su **OK**:

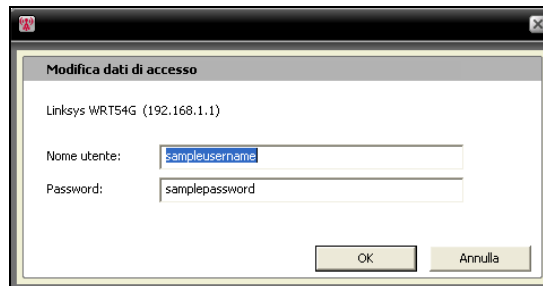
Impostazione	Descrizione
Rete	Nome della rete. Se si sta modificando una rete, non è possibile cambiarne il nome.
Impostazioni protezione	Protezione della rete non protetta. Se l'adattatore senza fili non supporta la modalità selezionata, la connessione non è possibile. Le modalità di protezione comprendono: Disattivata, WEP aperta, WEP condivisa, WEP automatica, WPA-PSK, WPA2-PSK.
Modalità crittografia	Crittografia associata alla modalità di protezione selezionata. Le modalità di crittografia comprendono: WEP, TKIP, AES e TKIP+AES.

Modifica delle credenziali per dispositivi senza fili

È possibile cambiare il nome utente o la password per un dispositivo nel router o nel punto di accesso senza fili protetto. L'elenco dei dispositivi viene visualizzato in **Dispositivi di rete senza fili protetti**.

McAfee consiglia di cambiare le credenziali perché la maggior parte dei dispositivi senza fili realizzati da un singolo produttore possiede le stesse credenziali di accesso. La modifica delle credenziali di accesso aiuta a impedire che altri accedano al proprio router o punto di accesso senza fili e ne modifichino le impostazioni.

Per cambiare il nome utente o la password per un dispositivo di rete senza fili protetto:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza configurazione**.
3. Nel riquadro Protezione rete, in **Dispositivi di rete senza fili protetti**, selezionare un router o un punto di accesso senza fili, quindi fare clic su **Cambia nome utente o password**.

4. Fare clic su **OK** nella finestra di dialogo Wireless Network Security dopo aver immesso le informazioni di accesso.

   Il nuovo nome utente e la nuova password vengono visualizzati in **Dispositivi di rete senza fili protetti**.

Nota: alcuni router non supportano nomi utente e pertanto un nome utente non verrà visualizzato in **Dispositivi di rete senza fili protetti**.

Ripristino delle impostazioni di protezione della rete

In caso di problemi con le impostazioni o la configurazione della protezione, è possibile utilizzare Wireless Network Security per ripristinare le impostazioni del router o del punto di accesso.

Per ripristinare le impostazioni di protezione:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza strumenti**.
3. Nel riquadro Strumenti, fare clic su **Strumenti di manutenzione**.
4. In **Riparazione delle impostazioni di protezione della rete** fare clic su **Ripristina**.
5. Nel riquadro Riparazione delle impostazioni di protezione della rete fare clic su **Ripristina**.

   Un avviso Wireless Network Security indica se la rete è stata ripristinata.

Nota: se il tentativo di ripristino della rete non riesce, connettersi alla rete utilizzando un cavo quindi ritentare. Se la password del router o del punto di accesso è cambiata, è necessario reimmetterla per connettersi.

Amministrazione delle chiavi di rete

Wireless Network Security genera chiavi di crittografia lunghe, complesse e casuali con un generatore di chiavi casuale. Con WEP, la chiave viene convertita in un valore esadecimale di 26 cifre (per 104 bit di entropia, o complessità, la complessità massima supportata da WEP a 128 bit), mentre con WPA, la chiave è una stringa ASCII di 63 caratteri. Ogni carattere ha 64 valori possibili (6 bit), per un totale di 384 bit di entropia, che supera la complessità della chiave WAP di 256 bit.

Quando si gestiscono chiavi di rete, è possibile visualizzarle in testo normale o con asterischi per punti di accesso non protetti, eliminare le chiavi salvate per punti di accesso non protetti, attivare o disattivare la rotazione delle chiavi, cambiare la frequenza di rotazione delle chiavi, ruotare manualmente la chiave e sospendere la rotazione delle chiavi.

Quando le chiavi ruotano automaticamente, gli strumenti degli hacker non sono in grado di acquisire le informazioni dell'utente perché la chiave cambia continuamente.

Tuttavia, se ci si connette a dispositivi senza fili che non sono supportati da Wireless Network Security (ad esempio quando si connette un palmare senza fili alla rete), è necessario annotare la chiave, arrestare la rotazione delle chiavi e quindi immetterla nel dispositivo.

Visualizzazione delle chiavi correnti

Wireless Network Security fornisce un accesso rapido alle informazioni di protezione senza fili, compresa la chiave corrente per una rete senza fili protetta.

Per visualizzare la chiave corrente:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza stato**.
3. Nel riquadro Stato rete senza fili, sotto il riquadro Rete senza fili protetta, fare clic su **Chiave corrente**.

   La chiave configurata per la rete viene visualizzata nella finestra di dialogo Configurazione chiave.

Argomenti correlati

- **Visualizzazione del numero di rotazioni delle chiavi** (pagina 134)

Rotazione automatica delle chiavi

Per impostazione predefinita, la rotazione automatica delle chiavi è attivata. Tuttavia, se viene sospesa un computer con accesso con privilegi di amministratore può riattivarla in seguito.

È possibile configurare Wireless Network Security in modo da ruotare automaticamente la chiave di protezione della rete senza fili.

Wireless Network Security genera automaticamente una serie infinita di chiavi complesse, che vengono sincronizzate attraverso la rete. La connessione senza fili può essere brevemente interrotta quando il router senza fili esegue il riavvio con la nuova configurazione della chiave di protezione, ma in genere questo non viene rilevato dagli utenti della rete.

Se alla rete non è connesso alcun computer, la rotazione delle chiavi ha luogo dopo la connessione del primo computer.

Per attivare la rotazione automatica delle chiavi:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza configurazione**.
3. Nel riquadro Protezione rete, selezionare **Attiva rotazione automatica delle chiavi.**

   È anche possibile riprendere la rotazione delle chiavi dal riquadro Stato rete senza fili.
4. Fare clic su **Applica**.

Nota: per impostazione predefinita, la rotazione delle chiavi ha luogo automaticamente ogni tre ore, ma è possibile regolare la frequenza in base ai propri requisiti di protezione.

Argomenti correlati

- **Regolazione della frequenza di rotazione delle chiavi** (pagina 115)
- **Ripresa della rotazione delle chiavi** (pagina 115)
- **Visualizzazione del numero di rotazioni delle chiavi** (pagina 134)

Ripresa della rotazione delle chiavi

Sebbene per impostazione predefinita la rotazione automatica delle chiavi sia attivata, un computer con accesso con privilegi di amministratore può riprenderla dopo averla sospesa.

Per riprendere la rotazione delle chiavi:

1 Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.

2 Selezionare **Visualizza stato**.

3 Nel riquadro Stato rete senza fili, fare clic su **Riprendi rotazione chiavi**.

   Gli avvisi Rotazione delle chiavi attivata e Chiave di protezione rotata confermano che la rotazione delle chiavi è stata avviata e che è stata completata correttamente.

Argomenti correlati

- **Rotazione automatica delle chiavi** (pagina 114)
- **Sospensione della rotazione automatica delle chiavi** (pagina 117)
- **Visualizzazione del numero di rotazioni delle chiavi** (pagina 134)

Regolazione della frequenza di rotazione delle chiavi

Se Wireless Network Security è configurato per ruotare automaticamente la chiave di protezione di una rete senza fili protetta, è possibile regolare l'intervallo di rotazione tra quindici minuti e quindici giorni.

McAfee consiglia una rotazione giornaliera.

Per regolare la frequenza di rotazione automatica delle chiavi:

1 Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.

2 Selezionare **Visualizza configurazione**.

3 Nel riquadro Protezione rete, controllare che la rotazione delle chiavi sia attivata, quindi spostare il cursore **Frequenza** su una delle seguenti impostazioni:

   - **ogni 15 minuti**
   - **ogni 30 minuti**
   - **ogni 1 ora**
   - **ogni 3 ore**

- **ogni 12 ore**
- **ogni 1 giorno**
- **ogni 7 giorni**
- **ogni 15 giorni**

4 Fare clic su **Applica**.

Nota: controllare che la rotazione automatica delle chiavi sia attivata prima di impostarne la frequenza.

Argomenti correlati

- **Attivazione della rotazione automatica delle chiavi** (pagina 114)
- **Visualizzazione del numero di rotazioni delle chiavi** (pagina 134)

Sospensione della rotazione automatica delle chiavi

La rotazione delle chiavi può essere sospesa da qualsiasi computer connesso alla rete senza fili. Si potrebbe voler sospendere la rotazione delle chiavi per:

- Consentire a un ospite, nel cui computer non è installato Wireless Network Security, di accedere alla rete
- Consentire a un sistema non Windows, ad esempio Macintosh, Linux o TiVo, di ottenere l'accesso. Dopo l'interruzione della rotazione delle chiavi, annotare la chiave e immetterla nel nuovo dispositivo.
- Consentire una connessione senza fili che non venga interrotta dalle rotazioni delle chiavi per certi programmi quali i giochi on-line.
- Si consiglia di riprendere la rotazione automatica delle chiavi appena si è in grado di garantire la completa protezione della rete dagli hacker.

Per visualizzare la chiave corrente:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza stato**.
3. Nel riquadro Stato rete senza fili, sotto il riquadro Rete senza fili protetta, fare clic su **Chiave corrente**. Annotare la chiave visualizzata nella finestra di dialogo Configurazione chiave. Altri computer in cui non è installato Wireless Network Security possono utilizzare questa chiave per connettersi alla rete senza fili protetta.
4. Nella finestra di dialogo Configurazione chiave fare clic su **Sospendi rotazione chiavi**.
5. Nella finestra di dialogo Rotazione delle chiavi sospesa fare clic su **OK** per continuare a lavorare.

Attenzione: se la rotazione delle chiavi non viene sospesa, i dispositivi senza fili non supportati che vengono connessi manualmente alla rete si disconnettono quando la chiave ruota.

È possibile creare un disco Windows Connect Now e utilizzare successivamente il file di testo per copiare e incollare la chiave nell'altro computer e dispositivo.

Argomenti correlati

- **Attivazione della rotazione automatica delle chiavi** (pagina 114)

- **Aggiunta di computer utilizzando la tecnologia Windows Connect Now** (pagina 90)
- **Ripresa della rotazione delle chiavi** (pagina 115)
- **Rotazione automatica delle chiavi** (pagina 114)
- **Visualizzazione del numero di rotazioni delle chiavi** (pagina 134)

Rotazione manuale delle chiavi di rete

Wireless Network Security consente di ruotare manualmente una chiave di rete anche se è attivata la rotazione automatica.

Per ruotare manualmente una chiave di rete:

1. Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Selezionare **Visualizza strumenti**.
3. Nel riquadro Strumenti, fare clic su **Strumenti di manutenzione**.
4. Nella pagina Strumenti di manutenzione, in **Rotazione manuale delle chiavi di protezione**, fare clic su **Esegui rotazione**.

   Viene visualizzato l'avviso Rotazione delle chiavi attivata che conferma l'inizio della rotazione. Dopo la rotazione delle chiavi di protezione, viene visualizzato l'avviso Chiave di protezione rotata che conferma che la rotazione delle chiavi ha avuto esito positivo.

Nota: per agevolare la manutenzione delle chiavi di protezione, è possibile attivare automaticamente la rotazione delle chiavi nel riquadro Protezione rete.

Se alla rete senza fili non è connesso alcun computer, la rotazione delle chiavi ha luogo automaticamente dopo la connessione del primo computer.

Argomenti correlati

- **Attivazione della rotazione automatica delle chiavi** (pagina 114)
- **Regolazione della frequenza di rotazione delle chiavi** (pagina 115)
- **Visualizzazione del numero di rotazioni delle chiavi** (pagina 134)

Visualizzazione delle chiavi come asterischi

Per impostazione predefinita le chiavi vengono visualizzate come asterischi ma è possibile configurare Wireless Network Security per visualizzarle in testo normale nelle reti che non sono protette da Wireless Network Security.

Le reti protette da Wireless Network Security visualizzano la chiave in testo normale.

Per visualizzare le chiavi come asterischi:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza configurazione**.
3. Fare clic su **Altre impostazioni**.
4. Deselezionare la casella **Visualizza chiavi in testo normale**.
5. Fare clic su **Applica**.

Argomenti correlati

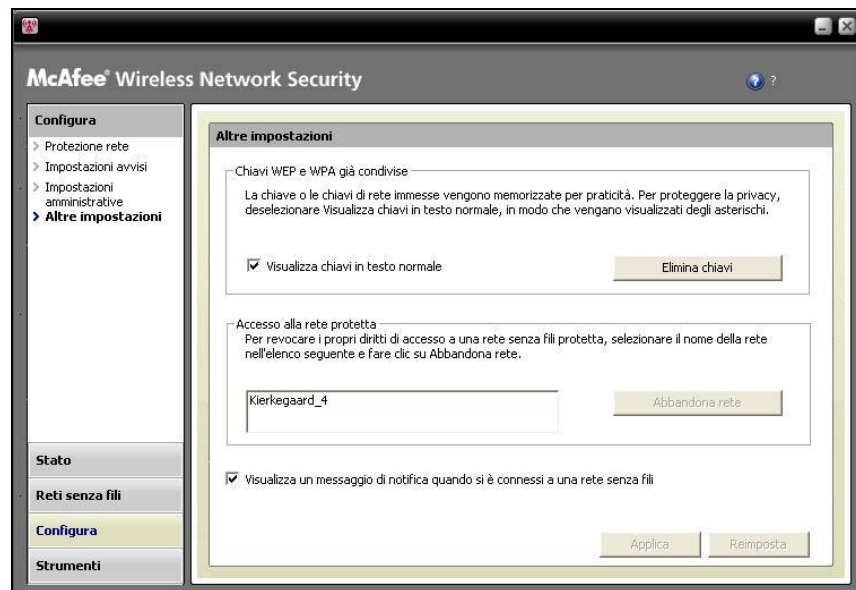
- **Visualizzazione delle chiavi in testo normale** (pagina 120)

Visualizzazione delle chiavi in testo normale

Per impostazione predefinita le chiavi vengono visualizzate come asterischi ma è possibile configurare Wireless Network Security per visualizzarle in testo normale nelle reti che non sono protette da Wireless Network Security.

Le reti protette da Wireless Network Security visualizzano la chiave in testo normale.

Per visualizzare le chiavi in testo normale:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza configurazione**.
3. Fare clic su **Altre impostazioni**.

4. Selezionare la casella **Visualizza chiavi in testo normale**.
5. Fare clic su **Applica**.

Argomenti correlati

- **Visualizzazione delle chiavi come asterischi** (pagina 119)

Eliminazione delle chiavi di rete

Wireless Network Security salva automaticamente le chiavi WEP e WPA già condivise, che possono essere eliminate in qualsiasi momento.

Per eliminare tutte le chiavi di rete:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza configurazione**.
3. Nel riquadro **Configura**, fare clic su **Altre impostazioni**.
4. Nel riquadro **Altre impostazioni**, in **Chiavi WEP e WPA già condivise**, fare clic su **Elimina chiavi**.
5. Nella finestra di dialogo Cancella chiavi, fare clic su **Sì** se si è certi di voler eliminare tutte le chiavi WEP e WPA memorizzate già condivise.

Attenzione: le chiavi eliminate vengono rimosse definitivamente dal computer. Dopo aver eliminato le chiavi di rete è necessario immettere la chiave corretta per connettersi a una rete WEP e WPA.

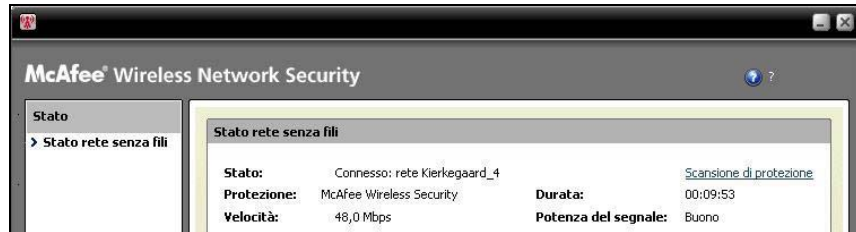
CAPITOLO 17

Monitoraggio delle reti senza fili

Wireless Network Security consente di monitorare lo stato della rete senza fili e dei computer protetti.

In questo capitolo

Monitoraggio delle connessioni di rete senza fili

È possibile visualizzare lo stato della connessione di rete, la modalità di protezione, la velocità, la durata, la potenza del segnale e un rapporto sulla protezione nel riquadro Stato rete senza fili.

Nella tabella seguente vengono descritti gli indicatori di stato per le connessioni di rete senza fili.

Stato	Descrizione	Informazioni
Stato	Visualizza se il computer è connesso a una rete e a quale	**Visualizzazione dello stato della connessione** (pagina 126)
Protezione	Visualizza la modalità di protezione della rete alla quale si è connessi. Se la protezione è assicurata da Wireless Network Security, viene visualizzato Wireless Network Security.	**Visualizzazione della modalità di protezione della rete** (pagina 128)
Velocità	Visualizza la velocità di connessione del computer alla rete.	**Visualizzazione della velocità di connessione alla rete** (pagina 128)
Durata	Visualizza per quanto tempo il computer è stato connesso alla rete.	**Visualizzazione della durata della connessione di rete** (pagina 129)

Potenza del segnale	Visualizza la potenza relativa del segnale della rete.	**Visualizzazione della potenza del segnale della rete** (pagina 131)
Scansione di protezione	Facendo clic su **Ricerca protezione** vengono visualizzate le informazioni di protezione, ad esempio le vulnerabilità della protezione senza fili, i problemi di prestazioni e lo stato della rete senza fili.	**Visualizzazione del rapporto sulla protezione on-line** (pagina 131)

Argomenti correlati

- **Informazioni sulle icone di Wireless Network Security** (pagina 94)

Visualizzazione dello stato della connessione

È possibile utilizzare il riquadro Stato rete senza fili per verificare lo stato della connessione di rete, per controllare se si è connessi o disconnessi dalla rete.

Per visualizzare lo stato di connessione senza fili:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza stato**.

   I computer connessi alla rete senza fili protetta e la data e l'ora di connessione di ognuno di essi vengono visualizzati nel riquadro Stato rete senza fili, in **Computer**.

Argomenti correlati

- **Monitoraggio delle connessioni di rete senza fili** (pagina 124)
- **Visualizzazione della modalità di protezione della rete** (pagina 128)
- **Visualizzazione della velocità di connessione alla rete** (pagina 128)
- **Visualizzazione della durata della connessione di rete** (pagina 129)
- **Visualizzazione della potenza del segnale della rete** (pagina 131)
- **Visualizzazione del rapporto sulla protezione on-line** (pagina 131)

Visualizzazione della modalità di protezione della rete

È possibile utilizzare il riquadro Stato rete senza fili per verificare la modalità di protezione della connessione di rete.

Per visualizzare la modalità di protezione della rete:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza stato**.

   La modalità di protezione viene visualizzata nel riquadro Stato rete senza fili nella casella **Protezione**.

   Se la rete senza fili è protetta da Wireless Network Security, viene visualizzato Wireless Network Security.

Argomenti correlati

- **Monitoraggio delle connessioni di rete senza fili** (pagina 124)
- **Visualizzazione dello stato della connessione** (pagina 126)
- **Visualizzazione della velocità di connessione alla rete** (pagina 128)
- **Visualizzazione della durata della connessione di rete** (pagina 129)
- **Visualizzazione della potenza del segnale della rete** (pagina 131)
- **Visualizzazione del rapporto sulla protezione on-line** (pagina 131)

Visualizzazione della velocità di connessione alla rete

È possibile utilizzare il riquadro Stato rete senza fili per verificare la velocità della connessione del computer alla rete.

Per visualizzare la velocità di connessione alla rete:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza stato**.

   La velocità di connessione viene visualizzata nel riquadro Stato rete senza fili nella casella **Velocità**.

Argomenti correlati

- **Monitoraggio delle connessioni di rete senza fili** (pagina 124)
- **Visualizzazione dello stato della connessione** (pagina 126)
- **Visualizzazione della modalità di protezione della rete** (pagina 128)
- **Visualizzazione della durata della connessione di rete** (pagina 129)
- **Visualizzazione della potenza del segnale della rete** (pagina 131)
- **Visualizzazione del rapporto sulla protezione on-line** (pagina 131)

Visualizzazione della durata della connessione di rete

È possibile utilizzare il riquadro Stato rete senza fili per verificare la durata della connessione alla rete.

Per visualizzare la durata della connessione alla rete:

1 Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.

2 Scegliere **Visualizza stato**.

   La durata della connessione del computer alla rete senza fili è visualizzata nella casella **Durata**.

Argomenti correlati

- **Monitoraggio delle connessioni di rete senza fili** (pagina 124)
- **Visualizzazione dello stato della connessione** (pagina 126)
- **Visualizzazione della modalità di protezione della rete** (pagina 128)
- **Visualizzazione della velocità di connessione alla rete** (pagina 128)
- **Visualizzazione della potenza del segnale della rete** (pagina 131)
- **Visualizzazione del rapporto sulla protezione on-line** (pagina 131)

Visualizzazione della potenza del segnale della rete

È possibile utilizzare il riquadro Stato rete senza fili per verificare la potenza del segnale della rete.

Per visualizzare la potenza del segnale:

1 Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.

2 Scegliere **Visualizza stato**.

   La qualità del segnale viene visualizzata nella casella **Potenza del segnale**.

Argomenti correlati

- **Monitoraggio delle connessioni di rete senza fili** (pagina 124)
- **Visualizzazione dello stato della connessione** (pagina 126)
- **Visualizzazione della modalità di protezione della rete** (pagina 128)
- **Visualizzazione della velocità di connessione alla rete** (pagina 128)
- **Visualizzazione della durata della connessione di rete** (pagina 129)
- **Visualizzazione del rapporto sulla protezione on-line** (pagina 131)

Visualizzazione del rapporto sulla protezione on-line

È possibile utilizzare il riquadro Stato rete senza fili per visualizzare un rapporto sulla connessione senza fili, se è protetta o meno.

Nella pagina Web McAfee wi-fiscan sono visualizzate le informazioni sulle vulnerabilità della protezione senza fili, problemi di prestazioni, informazioni sulla connessione senza fili, una soluzione di protezione consigliata e viene indicato se la connessione è protetta.

Prima di visualizzare il rapporto sulla protezione, accertarsi di avere una connessione Internet.

Per visualizzare un rapporto sulla protezione on-line della rete:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza stato**.
3. Nel riquadro Stato rete senza fili, fare clic su **Ricerca protezione**.

   Dopo l'apertura del browser, è necessario scaricare e installare un componente ActiveX. In base alla sua configurazione, il browser può bloccare il controllo. Consentire al browser di scaricare il componente, quindi eseguirlo per iniziare la scansione. La durata della scansione varia in base alla velocità della connessione Internet.

Nota: per informazioni sul download di componenti ActiveX, vedere la documentazione del browser.

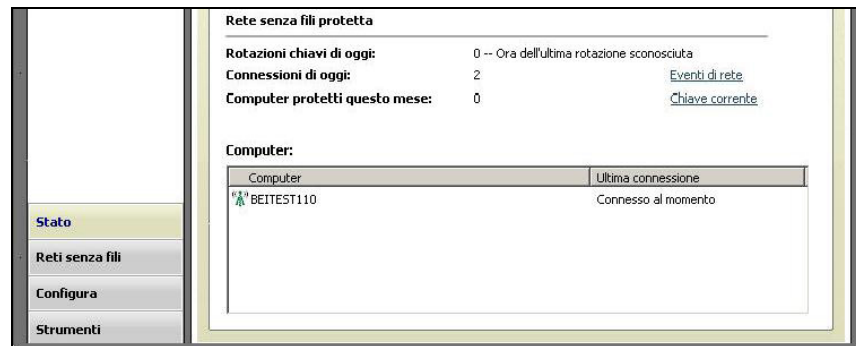
Wi-fiscan di McAfee supporta Internet Explorer 5.5 e versioni superiori.

Argomenti correlati

- **Monitoraggio delle connessioni di rete senza fili** (pagina 124)
- **Visualizzazione dello stato della connessione** (pagina 126)
- **Visualizzazione della modalità di protezione della rete** (pagina 128)
- **Visualizzazione della velocità di connessione alla rete** (pagina 128)
- **Visualizzazione della durata della connessione di rete** (pagina 129)

- **Visualizzazione della potenza del segnale della rete** (pagina 131)

Monitoraggio delle reti senza fili protette

Wireless Network Security consente di visualizzare il numero di connessioni, di rotazioni delle chiavi e di computer protetti nel riquadro Stato rete senza fili. È anche possibile visualizzare eventi di rete, la chiave corrente e i computer protetti attualmente.

Nella tabella seguente vengono descritti gli indicatori di stato per le connessioni di rete senza fili protette.

Stato	Descrizione	Informazioni
Rotazioni chiavi di oggi	Visualizza il numero quotidiano di rotazioni delle chiavi nella rete senza fili protetta.	**Visualizzazione del numero di rotazioni delle chiavi** (pagina 135)
Connessioni di oggi	Visualizza il numero quotidiano di connessioni alla rete protetta.	**Visualizzazione del numero di connessioni quotidiane** (pagina 136)
Computer protetti questo mese	Visualizza il numero di computer protetti per il mese corrente.	**Visualizzazione del numero di computer protetti mensilmente** (pagina 136)
Eventi di rete	Facendo clic su **Eventi di rete** vengono visualizzati gli eventi di rete, connessione e rotazione delle chiavi.	**Visualizzazione degli eventi di rete senza fili protetta** (pagina 136)

Computer	Visualizza il numero di computer connessi alla rete senza fili protetta e quando ogni computer si è connesso.	**Visualizzazione dei computer attualmente protetti** (pagina 138)

Visualizzazione del numero di rotazioni delle chiavi

Wireless Network Security consente di visualizzare il numero quotidiano di rotazioni delle chiavi che si sono verificate nella rete protetta e quando è avvenuta l'ultima.

Per visualizzare il numero quotidiano di rotazioni delle chiavi:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza stato**.

   Il numero totale di connessioni e la rotazione delle chiavi più recente sono visualizzati nel riquadro Stato rete senza fili, in **Rete senza fili protetta**, nel campo **Rotazioni chiavi di oggi**.

Argomenti correlati

- **Monitoraggio delle reti senza fili protette** (pagina 133)
- **Visualizzazione del numero di connessioni quotidiane** (pagina 136)
- **Visualizzazione del numero di computer protetti mensilmente** (pagina 136)
- **Visualizzazione degli eventi di rete senza fili protetta** (pagina 136)
- **Visualizzazione dei computer attualmente protetti** (pagina 138)
- **Amministrazione delle chiavi di rete** (pagina 113)
- **Rotazione automatica delle chiavi** (pagina 114)
- **Rotazione manuale delle chiavi di rete** (pagina 118)

Visualizzazione del numero di connessioni quotidiane

Wireless Network Security consente di visualizzare il numero quotidiano di connessioni alla rete protetta.

Per visualizzare le connessioni della rete senza fili protetta:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza stato**.

   Il numero totale di connessioni viene visualizzato nel riquadro Stato rete senza fili, in **Rete senza fili protetta**, nella casella **Connessioni di oggi**.

Argomenti correlati

- **Monitoraggio delle reti senza fili protette** (pagina 133)
- **Visualizzazione del numero di computer protetti mensilmente** (pagina 136)
- **Visualizzazione degli eventi di rete senza fili protetta** (pagina 136)
- **Visualizzazione dei computer attualmente protetti** (pagina 138)

Visualizzazione del numero di computer protetti mensilmente

Wireless Network Security consente di visualizzare il numero di computer protetti per il mese corrente.

Per visualizzare il numero di computer protetti per il mese corrente:

1. Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.
2. Scegliere **Visualizza stato**.
3. Il numero di computer protetti durante il mese corrente viene visualizzato nel riquadro Stato rete senza fili, in **Rete senza fili protetta**, nella casella **Computer protetti questo mese**.

Argomenti correlati

- **Monitoraggio delle reti senza fili protette** (pagina 133)
- **Visualizzazione del numero di rotazioni delle chiavi** (pagina 135)
- **Visualizzazione del numero di connessioni quotidiane** (pagina 136)
- **Visualizzazione degli eventi di rete senza fili protetta** (pagina 136)
- **Visualizzazione dei computer attualmente protetti** (pagina 138)

Visualizzazione degli eventi di rete senza fili protetta

Wireless Network Security registra eventi nella rete senza fili quali ad esempio il momento in cui le chiavi di protezione vengono ruotate, quando altri computer si connettono alla rete protetta da McAfee e quando altri computer vengono aggiunti alla rete protetta da McAfee.

Wireless Network Security consente di visualizzare un rapporto in cui sono descritti gli eventi che si sono verificati nella rete. È possibile specificare i tipi di eventi da visualizzare e ordinare le informazioni sugli eventi in base alla data, all'evento o al computer.

Per visualizzare gli eventi di rete:

1 Fare clic con il pulsante destro del mouse sull'icona di Wireless Network Security nell'area di notifica di Windows.

2 Effettuare una delle seguenti operazioni:

Per...	Procedere come segue...
Visualizzare gli eventi di rete dal riquadro Stato rete senza fili	1. Selezionare **Visualizza stato**. 2. Nel riquadro Stato rete senza fili, in **Rete senza fili protetta**, fare clic su **Eventi di rete**.
Visualizzare gli eventi di rete dal riquadro Stato rete senza fili	1. Fare clic su **Visualizza strumenti**. 2. Nel riquadro Strumenti, fare clic su **Strumenti di manutenzione**. 3. Nel riquadro Strumenti di manutenzione, in **Visualizzare registro eventi**, fare clic su **Visualizza**.

3 Selezionare uno o più degli eventi seguenti da visualizzare:

- **Eventi di rete**: Visualizza le informazioni sull'attività di rete, ad esempio la protezione di un router o di un punto di accesso senza fili.
- **Eventi di connessione**: Visualizza informazioni sulle connessioni di rete, ad esempio la data e l'ora in cui un computer si è connesso alla rete.
- **Eventi di rotazione chiave**: Visualizza informazioni sulle date e l'ora delle rotazioni delle chiavi di protezione.

4 Fare clic su **Chiudi**.

Argomenti correlati

- **Monitoraggio delle reti senza fili protette** (pagina 133)
- **Visualizzazione del numero di rotazioni delle chiavi** (pagina 135)
- **Visualizzazione del numero di connessioni quotidiane** (pagina 135)
- **Visualizzazione del numero di connessioni quotidiane** (pagina 136)
- **Visualizzazione dei computer attualmente protetti** (pagina 138)

Visualizzazione dei computer attualmente protetti

È possibile visualizzare il numero di computer connessi alla rete senza fili protetta e l'ultima connessione di ciascuno di essi.

Per visualizzare i computer connessi alla rete protetta:

1 Fare clic con il pulsante destro sull'icona di Wireless Network Security nell'area di notifica di Windows.

2 Scegliere **Visualizza stato**.

3 I computer connessi alla rete senza fili protetta e la data e l'ora dell'ultima connessione di ognuno di essi vengono visualizzati nel riquadro Stato rete senza fili, in **Computer**.

Argomenti correlati

- **Monitoraggio delle reti senza fili protette** (pagina 133)
- **Visualizzazione del numero di rotazioni delle chiavi** (pagina 135)
- **Visualizzazione del numero di connessioni quotidiane** (pagina 135)
- **Visualizzazione del numero di computer protetti mensilmente** (pagina 136)
- **Visualizzazione degli eventi di rete senza fili protetta** (pagina 136)

CAPITOLO 18

Risoluzione dei problemi

È possibile risolvere i problemi quando si utilizza Wireless Security e dispositivi di terzi, compreso quanto segue:

- Difficoltà di installazione
- Impossibilità di proteggere o configurare la rete
- Impossibilità di connettere i computer alla rete
- Impossibilità di connettersi a una rete o a Internet
- Altri problemi

In questo capitolo

Installazione di Wireless Network Security

È possibile risolvere i seguenti problemi di installazione.

- Su quali computer installare questo software
- Adattatore senza fili non rilevato
- Più adattatori senza fili
- Impossibile effettuare il download sui computer senza fili perché la rete è già protetta

Su quali computer installare questo software

Installare Wireless Network Security su ogni computer senza fili nella rete (a differenza di altri programmi McAfee, è possibile installare questo software su diversi computer). Rispettare il contratto di licenza del software acquistato. In alcuni casi potrebbe essere necessario acquistare licenze supplementari.

È possibile (ma non necessario) installarlo su computer che non dispongono di adattatori senza fili, ma il software non sarà attivo su tali computer perché non necessitano di protezione senza fili.

Wireless Network Security è attualmente supportato su Windows XP o Windows 2000.

Adattatore senza fili compatibile non rilevato

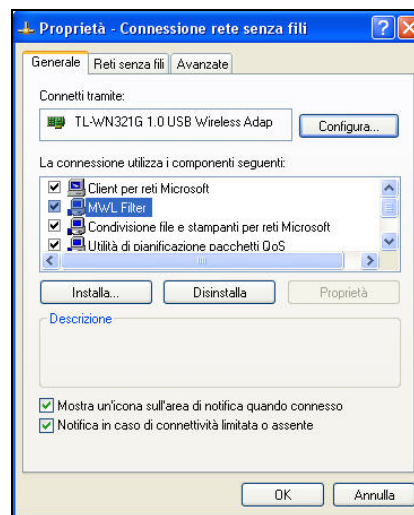
Se l'adattatore senza fili non viene rilevato al momento dell'installazione e dell'attivazione, riavviare il computer. Se l'adattatore continua a non essere rilevato dopo aver riavviato il computer, attenersi alla seguente procedura.

1 Avviare la finestra di dialogo Proprietà connessione senza fili di Windows.

2 Tramite il menu di avvio classico di Windows fare clic su **Start**, scegliere **Impostazioni**, quindi selezionare **Connessioni di rete**.

3 Fare clic sull'icona **Connessione rete senza fili**.

4 Nella finestra di dialogo Connessione rete senza fili - Stato, fare clic su **Proprietà**.

5 Nel riquadro Proprietà connessione senza fili deselezionare **Filtro MWL**, quindi riselezionarlo.

6 Fare clic su **OK**.

Se il problema permane, eseguire wi-fiscan. Se wi-fiscan funziona, l'adattatore è supportato. In caso contrario, aggiornare il driver dell'adattatore (utilizzare Windows Update o visitare il sito Web del produttore) oppure acquistare un nuovo dispositivo.

Argomenti correlati

- **Visualizzazione del rapporto sulla protezione on-line** (pagina 131)

Più adattatori senza fili

Se un messaggio di errore conferma che sono stati installati più adattatori senza fili, è necessario disattivarne o scollegarne uno. Wireless Home Network Security funziona esclusivamente con un solo adattatore senza fili.

Il download non riesce in una rete protetta

Se si dispone di un CD di installazione, installare Wireless Network Security dal CD su tutti i computer senza fili.

Se è stato installato il software su uno dei computer senza fili e la rete è stata protetta prima di installare il software su tutti gli altri computer senza fili, sono disponibili le seguenti opzioni.

- Rimuovere la protezione dalla rete. Quindi, scaricare il software e installarlo su tutti i computer senza fili. Proteggere di nuovo la rete.
- Visualizzare la chiave di rete. Quindi, immettere la chiave sul computer senza fili per connettersi alla rete. Scaricare e installare il software, quindi aggiungersi alla rete dal computer senza fili.
- Scaricare l'eseguibile sul computer già connesso alla rete e salvarlo su un'unità flash USB o scriverlo su un CD in modo da poterlo installare su altri computer.
- Eseguire la tecnologia Windows Connect Now.

Argomenti correlati

- **Rimozione di router o punti di accesso senza fili** (pagina 102)
- **Visualizzazione delle chiavi correnti** (pagina 113)
- **Aggiunta di computer tramite un dispositivo rimovibile** (pagina 88)
- **Aggiunta di computer utilizzando la tecnologia Windows Connect Now** (pagina 90)

Protezione o configurazione della rete

È possibile risolvere i seguenti problemi quando si protegge o configura la rete.

- Router o punto di accesso non supportato
- Aggiornare il firmware del router o del punto di accesso
- Errore di amministratore duplicato
- La rete risulta non protetta
- Impossibile ripristinare

Router o punto di accesso non supportato

Se un errore informa che il router o il punto di accesso senza fili non è supportato, Wireless Network Security non sarà stato in grado di configurare il dispositivo perché non l'ha rilevato o trovato.

Verificare di disporre della versione più recente di Wireless Network Security richiedendo un aggiornamento (McAfee aggiunge costantemente supporto per i nuovi router e punti di accesso). Se il router o il punto di accesso viene visualizzato nell'elenco dei router supportati e si riceve comunque questo errore, si stanno verificando errori di comunicazione tra il computer e il router o il punto di accesso

Argomenti correlati

- **Router senza fili supportati**
  http://www.mcafee.com/router

Aggiornare il firmware del router o del punto di accesso

Se un errore informa che il firmware del router o del punto di accesso senza fili non è supportato, il dispositivo in uso è supportato ma la revisione firmware del dispositivo non lo è. Verificare di disporre della versione più recente di Wireless Network Security richiedendo un aggiornamento (McAfee aggiunge costantemente supporto per le nuove revisioni firmware).

Se si dispone della versione più recente di Wireless Network Security, fare riferimento al sito Web del produttore o all'azienda di supporto per il router o il punto di accesso e installare una nuova versione del firmware presente nell'elenco dei router supportati.

Argomenti correlati

- **Router senza fili supportati**
  http://www.mcafee.com/router

Errore di amministratore duplicato

Dopo aver configurato il router o il punto di accesso, è necessario disconnettersi dall'interfaccia di amministrazione. A volte, in caso di mancata disconnessione, il router o il punto di accesso si comporta come se fosse in fase di configurazione tramite un altro computer. In tal caso viene visualizzato un messaggio di errore.

Se non è possibile disconnettersi, scollegare l'alimentazione dal router o dal punto di accesso, quindi ricollegarla.

Rotazione delle chiavi non riuscita

La rotazione della chiave non è riuscita perché:

- Le informazioni di accesso per il router o il punto di accesso sono state modificate.
- La versione firmware del router o del punto di accesso è stata modificata con una versione che non è supportata.
- Il router o il punto di accesso non è disponibile. Accertarsi che il router o il punto di accesso sia attivato e che sia connesso alla rete.
- Errore di duplicazione amministratore.
- Per alcuni router senza fili, se un altro computer viene collegato manualmente all'interfaccia Web del router senza fili il client McAfee potrebbe non essere in grado di accedere anche all'interfaccia di gestione per ruotare la chiave di crittografia.

Argomenti correlati

- **Modifica delle credenziali per dispositivi senza fili** (pagina 111)
- **Rotazione automatica delle chiavi** (pagina 114)

Impossibile ripristinare il router o il punto di accesso

Se non è possibile eseguire il ripristino, provare quanto riportato di seguito. Ciascuna delle seguenti procedure è indipendente.

- Connettersi alla rete utilizzando un cavo, quindi tentare nuovamente il ripristino.
- Scollegare l'alimentazione dal router o dal punto di accesso, ricollegarlo di nuovo, quindi tentare la connessione.
- Ripristinare le impostazioni predefinite del router o del punto di accesso, quindi eseguire il ripristino. In tal modo vengono ripristinate le impostazioni senza fili originali. Ripristinare quindi le impostazioni della connessione Internet.
- Utilizzare le opzioni avanzate, disconnettere tutti i computer dalla rete e ripristinare le impostazioni predefinite del router o del punto di accesso senza fili, quindi attivare la protezione. In tal modo vengono ripristinate le impostazioni senza fili originali. Ripristinare quindi le impostazioni della connessione Internet.

Argomenti correlati

- **Ripristino delle impostazioni di protezione della rete** (pagina 112)

La rete viene indicata come non protetta

Se viene indicato che la rete non è protetta, significa che la protezione non è attiva. È necessario proteggerla per renderla sicura. Wireless Network Security funziona solo con router e punti di accesso compatibili.

Argomenti correlati

- **Creazione di reti senza fili protette** (pagina 78)
- **Router senza fili supportati** http://www.mcafee.com/router

Connessione di computer a una rete

È possibile risolvere i seguenti problemi quando si connettono i computer alla rete.

- In attesa di autorizzazione
- Autorizzazione dell'accesso a un computer sconosciuto

In attesa di autorizzazione

Se si tenta di aggiungersi a una rete protetta e il computer resta nella modalità di attesa dell'autorizzazione, verificare quanto segue.

- Un computer senza fili che dispone già dell'accesso alla rete è acceso e connesso alla rete.
- È presente qualcuno per concedere l'accesso al computer quando viene visualizzato.
- I computer si trovano nel raggio di azione senza fili reciproco.

Se **Consenti accesso** non viene visualizzato sul computer che già dispone dell'accesso alla rete, provare a concedere l'accesso da un altro computer.

Se non sono disponibili altri computer, rimuovere la protezione della rete dal computer che già dispone dell'accesso e proteggere la rete dal computer che non disponeva dell'accesso. Quindi, aggiungersi alla rete dal computer che inizialmente proteggeva la rete.

È anche possibile utilizzare la funzione Proteggi un altro computer.

Argomenti correlati

- **Aggiunta a una rete senza fili protetta** (pagina 80)
- **Abbandono di reti senza fili protette** (pagina 105)
- **Rimozione di router o punti di accesso senza fili** (pagina 102)
- **Aggiunta di computer alla rete senza fili protetta** (pagina 88)

Autorizzazione dell'accesso a un computer sconosciuto

Quando da un computer sconosciuto si riceve una richiesta di concessione dell'accesso, negarla finché non è possibile verificarne la legittimità. Potrebbe trattarsi di un tentativo di accesso illegittimo alla rete.

Connessione a Internet e alla rete

È possibile risolvere i seguenti problemi quando ci si connette a una rete o a Internet.

- Connessione a Internet non valida
- Interruzione momentanea della connessione
- Perdita della connessione sui dispositivi (diversi dal proprio computer)
- Richiesta di immissione della chiave WEP, WPA o WPA2
- Impossibile connettersi
- Aggiornare l'adattatore senza fili
- Livello del segnale debole
- Windows non è in grado di configurare la connessione senza fili
- Windows non visualizza alcuna connessione

Impossibile connettersi a Internet

Se non è possibile connettersi, tentare di accedere alla rete utilizzando un cavo, quindi connettersi a Internet. Se ancora non è possibile connettersi, verificare quanto segue:

- Il modem è acceso
- Le impostazioni PPPoE sono corrette
- La linea DSL o via cavo è attiva

I problemi di connettività, quali la velocità e la potenza del segnale, possono essere causati anche da interferenze di altri dispositivi senza fili. Provare i seguenti metodi per risolvere il problema:

- Cambiare il canale del telefono cordless
- Eliminare le possibili fonti di interferenza
- Cambiare la posizione del punto di accesso, del computer o del router senza fili
- Cambiare il canale del router o del punto di accesso. Per il Nord America e il Sud America sono consigliati i canali 1, 4, 7 e 11. Per gli altri paesi sono consigliati i canali 1, 4, 7 e 13. Molti router sono impostati sul canale 6, per impostazione predefinita
- Controllare che il router e l'adattatore senza fili (in particolare un adattatore USB senza fili) non siano ostacolati da un muro
- Controllare che l'adattatore senza fili USB non si trovi accanto a un punto di accesso/router senza fili.
- Posizionare il router lontano da muri e metallo

Connessione interrotta

Quando la connessione si interrompe temporaneamente (ad esempio durante un gioco on-line), la causa potrebbe essere la rotazione delle chiavi. Per evitare che ciò accada, è possibile sospendere la rotazione delle chiavi.

Si consiglia di riprendere la rotazione delle chiavi non appena possibile per garantire la completa protezione della rete dagli hacker.

Argomenti correlati

- **Rotazione automatica delle chiavi** (pagina 114)
- **Ripresa della rotazione delle chiavi** (pagina 115)
- **Sospensione della rotazione automatica delle chiavi** (pagina 117)
- **Rotazione manuale delle chiavi di rete** (pagina 118)

I dispositivi perdono la connettività

Se alcuni dispositivi perdono la connettività quando si utilizza Wireless Network Security, provare a risolvere il problema utilizzando i seguenti metodi:

- Sospendere la rotazione delle chiavi
- Aggiornare il driver per l'adattatore senza fili
- Disattivare la gestione client dell'adattatore

Argomenti correlati

- **Sospensione della rotazione automatica delle chiavi** (pagina 117)

Richiesta di immissione della chiave WEP, WPA o WPA2

Se è necessario immettere una chiave WEP, WPA o WPA2 per collegarsi alla rete senza fili protetta, probabilmente il software non è stato installato sul computer.

Per il corretto funzionamento, è necessario che Wireless Network Security sia installato su ciascun computer senza fili nella rete.

Argomenti correlati

- **Avvio di Wireless Network Security** (pagina 72)
- **Aggiunta di computer alla rete senza fili protetta** (pagina 88)

Impossibile connettersi alla rete senza fili

Se ancora non è possibile connettersi, provare quanto riportato di seguito. Ciascuna delle seguenti procedure è indipendente.

- Se non si è collegati a una rete protetta, verificare di disporre della chiave corretta e immetterla nuovamente.
- Disconnettere l'adattatore senza fili, quindi connetterlo nuovamente oppure disattivarlo e riattivarlo nuovamente.
- Spegnere il router o il punto di accesso, accenderlo nuovamente, quindi tentare la connessione.
- Verificare che il router o il punto di accesso senza fili sia connesso e ripristinare le impostazioni di protezione.
- Riavviare il computer.
- Aggiornare l'adattatore senza fili o acquistarne uno nuovo. Ad esempio, se la rete utilizza la protezione WPA-PSK TKIP, l'adattatore senza fili potrebbe non supportare la modalità di protezione della rete (le reti visualizzano WEP, anche se sono state impostate su WPA).
- Se non è possibile connettersi dopo aver eseguito l'upgrade del router o del punto di accesso senza fili, potrebbe essere stato eseguito l'upgrade a una versione non supportata. Verificare che il router o il punto di accesso sia supportato. Se non fosse supportato, effettuare il downgrade a una versione supportata oppure attendere la disponibilità di un aggiornamento di Wireless Network Security.

Argomenti correlati

- **Ripristino delle impostazioni di protezione della rete** (pagina 112)
- **Aggiornamento dell'adattatore senza fili** (pagina 150)

Aggiornare l'adattatore senza fili

Potrebbe essere necessario aggiornare l'adattatore senza fili per poter utilizzare Wireless Network Security.

Per aggiornare l'adattatore:

1. Sul desktop, fare clic su **Start**, scegliere **Impostazioni**, quindi **Pannello di controllo**.
2. Fare doppio clic sull'icona **Sistema**. Verrà visualizzata la finestra di dialogo **Proprietà di sistema**.
3. Selezionare la scheda **Hardware**, quindi fare clic su **Gestione periferiche**.
4. Nell'elenco Gestione periferiche, fare doppio clic sull'adattatore.
5. Selezionare la scheda **Driver** e verificare il driver a disposizione.
6. Visitare il sito Web del produttore dell'adattatore per individuare un aggiornamento. I driver si trovano solitamente nella sezione Supporto o Download. Se si utilizza una scheda miniPCI, cercare nel sito del produttore del computer, non della scheda.
7. Se è disponibile l'aggiornamento di un driver, seguire le istruzioni riportate sul sito Web per effettuarne il download.
8. Tornare alla scheda **Driver**, quindi fare clic su **Aggiorna driver**. Verrà visualizzata una procedura guidata di Windows.
9. Per installare il driver, seguire le istruzioni riportate nel sito Web.

Livello del segnale debole

Se la connessione si interrompe o è lenta, il livello del segnale potrebbe non essere abbastanza potente. Per migliorare il segnale, provare quanto riportato di seguito:

- Verificare che i dispositivi senza fili non siano bloccati da oggetti metallici quali impianti di riscaldamento, condutture o apparecchi di grandi dimensioni. I segnali senza fili non passano attraverso questi oggetti.
- Se il segnale deve attraversare delle pareti, accertarsi che non debba attraversarle attraverso un angolo acuto Più è lungo il percorso attraverso una parete, più il segnale si indebolisce.
- Se il router o il punto di accesso senza fili dispone di più antenne, provare ad orientare le due antenne perpendicolarmente l'una all'altra (ad esempio, una verticale e l'altra orizzontale a un angolo di 90°).
- Alcuni produttori dispongono di antenne ad alto guadagno. Le antenne direzionali offrono un raggio d'azione più lungo, mentre le antenne omnidirezionali offrono maggiore versatilità. Consultare le istruzioni di installazione del produttore per effettuare l'installazione dell'antenna.

Se questa procedura non riesce, aggiungere un punto di accesso alla rete più vicino al computer al quale si sta tentando di connettersi. Se si configura il secondo punto di accesso con lo stesso nome di rete (SSID) e con un canale differente, l'adattatore individuerà automaticamente il segnale più potente e si collegherà attraverso il punto di accesso appropriato.

Argomenti correlati

- **Icone della potenza del segnale** (pagina 95)
- **Visualizzazione della potenza del segnale della rete** (pagina 130)

Windows non supporta la connessione senza fili

Ignorare eventuali messaggi di errore che informano che Windows non è in grado di configurare la connessione senza fili. Utilizzare Wireless Network Security per connettersi a reti senza fili e per configurarle.

Nella finestra di dialogo di Windows Proprietà connessione senza fili, nella scheda Reti senza fili, verificare che la casella **Usa Windows per configurare le impostazioni della rete senza fili** non sia selezionata.

Wireless Network Security consente:

- Agli adattatori installati in computer che eseguono Windows 2000 di connettersi a reti WPA, anche se la gestione client della scheda non è supportata.
- Agli adattatori in computer che eseguono Windows XP di connettersi a reti WPA2 senza dover trovare e installare l'aggiornamento rapido di Win XP SP2
- Agli adattatori sotto Windows XP SP1 di connettersi alle reti WPA e WPA2 senza dover individuare e installare un aggiornamento rapido, che non è supportato da Windows XP SP1.

Windows non visualizza alcuna connessione

Se si stabilisce una connessione, ignorare l'icona di rete di Windows in caso presenti una X (nessuna connessione). Si è stabilita una buona connessione.

Altri problemi

È possibile risolvere i seguenti problemi.

- Nome di rete differente durante l'utilizzo di altri programmi
- Problemi di configurazione dei router o dei punti di accesso senza fili
- Sostituzione di computer
- Selezionare un'altra modalità di protezione
- Software non funzionante in seguito all'aggiornamento dei sistemi operativi

Nome di rete differente durante l'utilizzo di altri programmi

Se il nome della rete è diverso quando viene visualizzato tramite altri programmi (ad esempio, _SafeAaf è parte del nome) non c'è da preoccuparsi.

Wireless Network Security contrassegna le reti con un codice quando sono protette.

Configurazione di router o punti di accesso senza fili

Se si verifica un errore durante la configurazione del router o del punto di accesso o durante l'aggiunta di più router sulla rete, verificare che tutti i router o i punti di accesso presentino un indirizzo IP distinto.

Se il nome del router o del punto di accesso senza fili viene visualizzato nella finestra di dialogo Proteggi router o access point, ma si verifica un errore durante la configurazione, verificare che il router o il punto di accesso sia supportato.

Se il router o il punto di accesso è configurato, ma non sembra essere sulla rete corretta (ad esempio, non vengono visualizzati altri computer collegati alla LAN), verificare di aver configurato il router o il punto di accesso appropriato. Scollegare l'alimentazione dal router o dal punto di accesso e verificare che la connessione venga interrotta. Se è stato configurato il router o il punto di accesso errato, rimuovere la protezione e applicarla al router o al punto di accesso corretto.

Se è impossibile configurare o aggiungere il router o il punto di accesso, ma si è sicuri che è supportato, alcune modifiche apportate potrebbero impedirne la corretta configurazione.

- Seguire le indicazioni del produttore per configurare il router o il punto di accesso senza fili per il DHCP o per configurare il corretto indirizzo IP. In alcuni casi, il produttore fornisce uno strumento di configurazione.
- Ripristinare le impostazioni di fabbrica del router o del punto di accesso e provare nuovamente a ripristinare la rete. La porta di amministrazione potrebbe essere stata modificata oppure l'amministrazione senza fili potrebbe essere stata disattivata. Verificare che venga utilizzata la configurazione predefinita e che la configurazione senza fili sia attivata. Un'altra possibilità è che l'amministrazione http sia disattivata. In questo caso, verificare che l'amministrazione http sia attivata. Accertarsi che sia utilizzata la porta 80 per l'amministrazione.
- Se il router o il punto di accesso senza fili non viene visualizzato nell'elenco dei router o dei punti di accesso senza fili che è possibile proteggere o ai quali è possibile connettersi, attivare la trasmissione SSID e verificare che il router o il punto di accesso sia presente nell'elenco delle reti senza fili disponibili di Wireless Network Security.
- Se si viene disconnessi o è impossibile stabilire una connessione, la causa potrebbe derivare dall'attivazione dei filtri MAC. Disattivare i filtri MAC.
- Se non è possibile eseguire operazioni di rete (ad esempio, condividere file o eseguire la stampa su stampanti condivise) tra due computer connessi alla rete senza fili, verificare di non aver attivato l'isolamento del punto di accesso. L'isolamento

del punto di accesso impedisce che i computer senza fili vengano connessi tra di loro tramite la rete.

- Se si utilizza un programma firewall diverso da McAfee Personal Firewall, accertarsi che la sottorete sia inserita fra quelle affidabili (trusted).

Argomenti correlati

- **Router senza fili supportati** http://www.mcafee.com/router

Sostituzione di computer

Se il computer che gestisce la protezione della rete viene sostituito e non esistono altri computer che dispongono dell'accesso (è impossibile accedere alla rete), ripristinare le impostazioni di fabbrica del router o del punto di accesso senza fili e applicare di nuovo la protezione sulla rete.

Selezionare un'altra modalità di protezione

Se un messaggio di errore informa che la modalità di protezione selezionata non è supportata dall'adattatore senza fili, è necessario selezionarne una diversa.

- Tutti gli adattatori supportano WEP.
- La maggior parte degli adattatori che supportano WPA implementa entrambe le modalità di protezione WPA-PSK TKIP e WPA-PSK AES.
- Gli adattatori che supportano WPA2 implementano le modalità di protezione WPA e WPA2-PSK TKIP, WPA2-PSK AES e WPA2-PSK TKIP/AES.

Argomenti correlati

- **Configurazione delle impostazioni di protezione** (pagina 108)
- **Visualizzazione della modalità di protezione della rete** (pagina 127)

Errore del software dopo l'aggiornamento dei sistemi operativi

Se Wireless Network Security non funziona dopo l'aggiornamento dei sistemi operativi, rimuovere e reinstallare il programma.

CAPITOLO 19

McAfee EasyNetwork

McAfee® EasyNetwork consente la condivisione protetta di file, semplifica i trasferimenti di file e automatizza la condivisione delle stampanti tra computer della rete domestica.

Prima di iniziare a utilizzare EasyNetwork, è opportuno acquisire dimestichezza con alcune delle funzioni più comuni. I dettagli relativi alla configurazione e all'utilizzo di queste funzioni sono reperibili nella Guida in linea di EasyNetwork.

In questo capitolo

Funzioni

EasyNetwork fornisce le funzioni riportate di seguito.

Condivisione di file

EasyNetwork semplifica la condivisione dei file tra il computer in uso e gli altri computer della rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer membri della rete gestita (cioè che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri membri.

Trasferimento di file

È possibile inviare file ad altri computer purché siano membri della rete gestita. Nel momento in cui si riceve un file, esso viene visualizzato nella casella di EasyNetwork, un percorso di archiviazione temporaneo per tutti i file ricevuti da altri computer della rete.

Condivisione automatica di stampanti

Dopo che l'utente è diventato membro di una rete gestita, EasyNetwork condivide automaticamente tutte le stampanti locali collegate al computer in uso, utilizzando il nome corrente della stampante come nome della stampante condivisa, rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso.

CAPITOLO 20

Impostazione di EasyNetwork

Prima di poter utilizzare le funzioni di EasyNetwork è necessario avviare il programma e diventare membro della rete gestita. Successivamente, sarà possibile abbandonare la rete in qualsiasi momento.

In questo capitolo

Avvio di EasyNetwork

Per impostazione predefinita viene richiesto di avviare EasyNetwork immediatamente dopo l'installazione, per quanto sia anche possibile avviarlo in un secondo momento.

Avvio di EasyNetwork

Per impostazione predefinita viene richiesto di avviare EasyNetwork immediatamente dopo l'installazione, benché sia anche possibile avviarlo in un secondo momento.

Per avviare EasyNetwork:

- Nel menu **Start**, scegliere **Programmi**, quindi **McAfee** e fare clic su **McAfee EasyNetwork**.

Suggerimento: se si decide di creare icone sul desktop e icone di avvio rapido durante l'installazione, è anche possibile avviare EasyNetwork facendo doppio clic sulla relativa icona sul desktop oppure, facendo un solo clic sull'icona McAfee EasyNetwork nell'area di notifica sulla destra della barra delle applicazioni.

Aggiunta di un membro alla rete gestita

Dopo aver installato SecurityCenter, un agente di rete viene aggiunto al computer ed eseguito in background. In EasyNetwork, l'agente di rete è responsabile del rilevamento di una connessione di rete valida, delle stampanti locali da condividere e del monitoraggio dello stato di rete.

Se non viene trovato nessun altro computer che esegue l'agente sulla rete a cui è connesso l'utente, quest'ultimo diventerà automaticamente membro della rete e gli verrà chiesto di stabilire se si tratta di rete affidabile. Poiché è il primo computer a diventare membro della rete, il nome del computer in uso viene incluso nel nome della rete, che potrà tuttavia essere rinominata in qualsiasi momento.

Quando un computer stabilisce una connessione alla rete, richiede agli altri computer attualmente in rete l'autorizzazione a diventarne membro. Alla richiesta è possibile acconsentire da qualsiasi computer con autorizzazioni amministrative in rete. La persona che concede le autorizzazioni può inoltre determinare il livello di autorizzazione del computer attualmente membro della rete, ad esempio, Guest (solo capacità di trasferimento file) oppure completo/con privilegi di amministratore (capacità di trasferimento e di condivisione file). In EasyNetwork, i computer che dispongono di accesso con privilegi di amministratore possono consentire l'accesso ad altri computer e gestire autorizzazioni (vale a dire, alzare o abbassare il livello dei computer) mentre i computer con accesso completo non sono in grado di eseguire attività amministrative di questo tipo. Prima di consentire al computer di diventare membro, viene anche eseguito un controllo di protezione.

Nota: una volta diventato membro di una rete, se sono stati installati altri programmi di rete McAfee (ad esempio, McAfee Wireless Network Security o Network Manager), il computer verrà anche riconosciuto come computer gestito in quei programmi. Il livello di autorizzazione assegnato al computer viene applicato a tutti i programmi di rete McAfee. Per ulteriori informazioni sul significato di autorizzazione guest, completa o con autorizzazioni amministrative in altri programmi di rete McAfee, consultare la relativa documentazione.

Aggiunta di un membro alla rete

Quando un computer si connette a una rete affidabile per la prima volta dopo l'installazione di EasyNetwork, viene visualizzato un messaggio che chiede al computer se intende diventare membro di una rete gestita. Se il computer accetta di diventarlo, verrà inviata una richiesta a tutti gli altri computer in rete che dispongono di accesso con privilegi di amministratore. Tale richiesta deve essere accettata prima che il computer possa condividere stampanti o file oppure inviare e copiare file in rete. Al primo computer della rete vengono automaticamente fornite autorizzazioni amministrative in rete.

Per diventare membro di una rete:

1. Nella finestra File condivisi, fare clic su **Sì, aggiungi il computer alla rete adesso**.
   Quando un computer con privilegi di amministratore in rete acconsente alla richiesta, viene visualizzato un messaggio in cui viene chiesto se si intende consentire al computer in uso e agli altri della rete di gestire le impostazioni di protezione reciproche.
2. Per consentire al computer in uso e agli altri computer di rete di gestire le reciproche impostazioni di protezione, fare clic su **Sì**, altrimenti fare clic su **No**.
3. Verificare che le carte da gioco visualizzate nella finestra di dialogo di conferma della protezione siano visualizzate anche sul computer a partire dal quale sono state concesse le autorizzazioni, quindi fare clic su **Conferma**.

Nota: se le stesse carte da gioco visualizzate nella finestra di dialogo di conferma della protezione non vengono visualizzate anche sul computer a partire dal quale sono state concesse le autorizzazioni, significa che si è verificata una violazione della protezione sulla rete gestita. Diventare membro della rete può mettere a rischio il proprio computer; pertanto, fare clic su **Rifiuta** nella finestra di dialogo di conferma.

Autorizzazione di accesso alla rete

Quando un computer chiede di diventare membro di una rete gestita, viene inviato un messaggio agli altri computer in rete che dispongono di accesso con privilegi di amministratore. Il primo computer a rispondere al messaggio diventa quello dell'utente che concede le autorizzazioni e, come tale, l'utente di questo computer sarà responsabile della scelta del tipo di accesso: Guest, completo o con privilegi di amministratore.

Per autorizzare l'accesso alla rete:

1 Nel messaggio di avviso, selezionare una delle seguenti caselle di controllo:
   - **Concedi accesso Guest**: consente all'utente di inviare file ad altri computer, ma non di condividerli.
   - **Concedi accesso completo a tutte le applicazioni della rete gestita**: consente all'utente di inviare e di condividere file.
   - **Concedi accesso con privilegi di amministratore a tutte le applicazioni della rete gestita**: consente all'utente di inviare e condividere file, autorizzare l'accesso ad altri computer e regolarne i livelli di autorizzazione.
2 Fare clic su **Consenti accesso**.
3 Verificare che le carte da gioco visualizzate nella finestra di dialogo di conferma della protezione siano visualizzate anche sul computer, quindi fare clic su **Conferma**.

Nota: se le stesse carte da gioco visualizzate nella finestra di dialogo di conferma della protezione non vengono visualizzate anche sul computer, significa che si è verificata una violazione della protezione sulla rete gestita. Poiché concedere a questo computer l'accesso alla rete potrebbe mettere a rischio il computer in uso, fare clic su **Rifiuta** nella finestra di dialogo di conferma della protezione.

Ridenominazione della rete

Per impostazione predefinita, il nome della rete include il nome del primo computer diventato membro della rete, tuttavia è possibile cambiarlo in qualsiasi momento. Quando si rinomina la rete, è possibile modificare la relativa descrizione visualizzata in EasyNetwork.

Per rinominare la rete:

1. Nel menu **Opzioni**, scegliere **Configura**.
2. Nella finestra di dialogo Configura, digitare il nome della rete nella casella **Nome di rete**.
3. Fare clic su **OK**.

Abbandono della rete gestita

Se l'utente diventato membro di una rete non intende più essere tale, può abbandonare la rete. Una volta che si è optato per l'abbandono è comunque possibile ridiventare membro della rete in qualsiasi momento, purché a tale scopo venga concessa l'autorizzazione e venga nuovamente effettuato un controllo di protezione. Per ulteriori informazioni, vedere **Aggiunta di un membro alla rete gestita** (pagina 159).

Abbandono della rete gestita

È possibile abbandonare una rete gestita di cui si è membri.

Per abbandonare una rete gestita:

1 Nel menu **Strumenti**, scegliere **Abbandona rete**.

2 Nella finestra di dialogo Abbandona rete, selezionare il nome della rete che si desidera abbandonare.

3 Fare clic su **Abbandona rete**.

CAPITOLO 21

Condivisione e invio di file

EasyNetwork semplifica la condivisione e l'invio di file sul computer in uso tra gli altri computer presenti in rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer membri della rete gestita (cioè che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri computer membri.

In questo capitolo

Condivisione di file

EasyNetwork semplifica la condivisione dei file tra il computer in uso e gli altri computer della rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer membri della rete gestita (cioè che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri computer membri. Se si condivide una cartella, vengono condivisi tutti i file in essa contenuti e le relative sottocartelle, tuttavia la condivisione delle cartelle aggiunte successivamente non avviene automaticamente. Una volta eliminati, file e cartelle condivisi vengono automaticamente rimossi dalla finestra File condivisi. È possibile interrompere la condivisione di un file in qualsiasi momento.

L'accesso a un file condiviso avviene in due modi: aprendo il file direttamente da EasyNetwork oppure copiandolo in una cartella del computer e quindi aprendolo. Se l'elenco dei file condivisi è troppo lungo, è possibile effettuare la ricerca dei file a cui si desidera accedere.

Nota: i file condivisi tramite EasyNetwork non sono accessibili da altri computer mediante Esplora risorse. La condivisione dei file EasyNetwork viene eseguita mediante connessioni protette.

Condivisione di un file

Quando si condivide un file, questo viene reso automaticamente disponibile a tutti gli altri membri che dispongono di accesso alla rete gestita, sia esso completo o con privilegi di amministratore.

Per condividere un file:

1. In Esplora risorse, individuare il file che si desidera condividere.
2. Trascinare il file dal percorso in Esplora risorse nella finestra File condivisi in EasyNetwork.

Suggerimento: è anche possibile condividere un file facendo clic su **Condividi file** nel menu **Strumenti**. Nella finestra di diaIogo Condividi, passare alla cartella in cui è memorizzato il file che si desidera condividere, selezionarlo e fare clic su **Condividi**.

Interruzione della condivisione di un file

Se un file viene condiviso sulla rete gestita, è possibile interrompere la condivisione in qualsiasi momento. Quando si interrompe la condivisione di un file, gli altri membri della rete gestita non possono più accedervi.

Per interrompere la condivisione di un file:

1. Nel menu **Strumenti**, scegliere **Interrompi condivisione file**.
2. Nella finestra di dialogo Interrompi condivisione file, selezionare il file che non si desidera più condividere.
3. Fare clic su **Non condividere**.

Copia di un file condiviso

È possibile copiare nel computer in uso i file condivisi provenienti da un qualsiasi computer della rete gestita. Si disporrà quindi ancora di una copia anche nel caso in cui il computer interrompa la condivisione del file.

Per copiare un file:

- Trascinare un file dalla finestra File condivisi di EasyNetwork in un percorso di Esplora risorse o sul desktop di Windows.

Suggerimento: è anche possibile copiare un file condiviso selezionandolo in EasyNetwork, quindi facendo clic su **Copia in** nel menu **Strumenti**. Nella finestra di dialogo Copia in, passare alla cartella in cui si desidera copiare il file, selezionarlo e fare clic su **Salva**.

Ricerca di un file condiviso

È possibile ricercare un file di cui si è eseguita la condivisione oppure che è stato condiviso da qualsiasi altro membro della rete. Nel momento in cui vengono digitati i criteri di ricerca, EasyNetwork visualizza automaticamente i risultati corrispondenti nella finestra File condivisi.

Per cercare un file condiviso:

1. Nella finestra File condivisi, fare clic su **Cerca**.
2. Scegliere una delle seguenti opzioni nell'elenco **Contiene**:
   - **Contiene tutte le parole**: consente di cercare i nomi di file o di percorso contenenti tutte le parole specificate nell'elenco **Nome file o percorso**, in qualsiasi ordine.
   - **Contiene una qualsiasi delle parole**: consente di cercare i nomi di file o di percorso contenenti una qualsiasi delle parole specificate nell'elenco **Nome file o percorso**.

- **Contiene la stringa esatta**: consente di cercare i nomi di file o di percorso contenenti esattamente la stringa specificata nell'elenco **Nome file o percorso**.

3 Digitare, tutto o in parte, il nome del file o del percorso nell'elenco **Nome file o percorso**.

4 Scegliere una delle seguenti opzioni nell'elenco **Tipo**:

- **Qualsiasi**: consente di cercare tutti i tipi di file condivisi.
- **Documento**: consente di cercare tutti i documenti condivisi.
- **Immagine**: consente di cercare tutti i file di immagine condivisi.
- **Video**: consente di cercare tutti i file video condivisi.
- **Audio**: consente di cercare tutti i file audio condivisi.

5 Negli elenchi **Da** e **A** , fare clic sulle date che rappresentano l'intervallo temporale in cui è stato creato il file.

Invio di file ad altri computer

È possibile inviare file ad altri computer purché siano membri della rete gestita. Prima di inviare un file, EasyNetwork verifica che il computer che lo riceve abbia sufficiente spazio su disco.

Nel momento in cui si riceve un file, esso viene visualizzato nella casella dei file in arrivo di EasyNetwork, un percorso di archiviazione temporaneo per tutti i file ricevuti da altri computer della rete. Se durante la ricezione EasyNetwork è aperto, il file viene immediatamente visualizzato nella casella dei file in arrivo, in caso contrario viene visualizzato un messaggio nell'area di notifica a destra della barra delle applicazioni di Windows. Se non si desidera ricevere messaggi di notifica è possibile disattivarli. Qualora nella casella dei file in arrivo esista già un file con lo stesso nome, il nuovo file viene rinominato con un suffisso numerico. I file restano nella casella finché l'utente li accetta, vale a dire finché vengono copiati in un percorso sul computer in uso.

Invio di un file a un altro computer

È possibile inviare un file direttamente a un altro computer della rete gestita senza condividerlo. Prima che un utente del computer destinatario possa visualizzare il file, sarà necessario salvarlo in un percorso locale. Per ulteriori informazioni, vedere **Accettazione di un file da un altro computer** (pagina 170).

Per inviare un file a un altro computer:

1 In Esplora risorse, individuare il file che si desidera inviare.

2 In EasyNetwork, trascinare il file dal percorso in Esplora risorse sull'icona di un computer attivo.

Suggerimento: è possibile inviare più file a un computer premendo CTRL mentre li si seleziona. Per inviare i file è inoltre possibile fare clic su **Invia** nel menu **Strumenti**, selezionare i file e fare clic su **Invia**.

Accettazione di un file proveniente da un altro computer

Se un altro computer della rete gestita invia un file all'utente, è necessario accettarlo (salvandolo in una cartella del computer). Se durante l'invio del file al computer in uso EasyNetwork non è aperto o non è in primo piano, l'utente riceverà un messaggio nell'area di notifica a destra della barra delle applicazioni. Fare clic sul messaggio di notifica per aprire EasyNetwork e accedere al file.

Per ricevere un file da un altro computer:

- Fare clic su **Ricevuto**, quindi trascinare il file dalla casella dei file in arrivo di EasyNetwork in una cartella di Esplora risorse.

Suggerimento: è anche possibile ricevere un file da un altro computer selezionandolo nella casella dei file in arrivo di EasyNetwork e facendo clic su **Accetta** nel menu **Strumenti**. Nella finestra di dialogo Accetta nella cartella, passare alla cartella in cui si desidera salvare i file in ricezione, effettuare la selezione e fare clic su **Salva**.

Ricezione di una notifica all'invio di un file

È possibile ricevere una notifica quando un altro computer della rete gestita invia un file. Se EasyNetwork al momento non è aperto o non è in primo piano sul desktop, verrà visualizzato un messaggio nell'area di notifica sulla destra della barra delle applicazioni.

Per ricevere una notifica all'invio di un file:

1. Nel menu **Opzioni**, scegliere **Configura**.
2. Nella finestra di dialogo Configura, selezionare la casella di controllo **Avvisa quando è in corso l'invio di file da altri computer**.
3. Fare clic su **OK**.

CAPITOLO 22

Condivisione di stampanti

Una volta che l'utente è diventato membro di una rete gestita, EasyNetwork condivide automaticamente qualsiasi stampante locale collegata al computer, rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso.

In questo capitolo

Uso delle stampanti condivise

Una volta che l'utente è diventato membro di una rete gestita, EasyNetwork condivide automaticamente tutte le stampanti locali collegate al computer in uso, utilizzando il nome corrente della stampante come nome della stampante condivisa, rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso. Se è stato configurato un driver per stampare mediante un server di stampa di rete (ad esempio, un server di stampa USB senza fili), EasyNetwork considera la stampante come locale e la condivide automaticamente in rete. È anche possibile interrompere la condivisione di una stampante in qualsiasi momento.

EasyNetwork rileva inoltre le stampanti condivise da tutti gli altri computer della rete. Se viene rilevata una stampante remota non ancora connessa al computer, quando EasyNetwork viene aperto per la prima volta, nella finestra File condivisi viene visualizzato il collegamento **Stampanti di rete disponibili**. In questo modo l'utente potrà installare le stampanti disponibili o disinstallare quelle già connesse al computer nonché aggiornare l'elenco delle stampanti rilevate sulla rete.

Se invece è connesso alla rete gestita ma non ne è ancora diventato membro, l'utente potrà accedere alle stampanti condivise mediante il normale pannello di controllo delle stampanti di Windows.

Interruzione della condivisione di una stampante

È possibile interrompere la condivisione di una stampante in qualsiasi momento. I membri che hanno già installato la stampante non potranno più stampare su di essa.

Per interrompere la condivisione di una stampante:

1. Nel menu **Strumenti**, scegliere **Stampanti**.
2. Nella finestra di dialogo Gestione stampanti di rete, fare clic sul nome della stampante che non si desidera più condividere.
3. Fare clic su **Non condividere**.

Installazione di una stampante di rete disponibile

Come membro di una rete gestita, è possibile accedere alle stampanti condivise in rete purché vengano installati i driver appropriati. Se il proprietario della stampante interrompe la condivisione dopo che l'utente ha effettuato l'installazione, non sarà più possibile stampare su quella stampante.

Per installare una stampante di rete disponibile:

1. Nel menu **Strumenti**, scegliere **Stampanti**.
2. Nella finestra di dialogo Stampanti di rete disponibili, fare clic sul nome di una stampante.
3. Fare clic su **Installa**.

CAPITOLO 23

Riferimento

Nel Glossario dei termini sono elencati e illustrati i termini relativi alla protezione più comunemente utilizzati nei prodotti McAfee.

In Informazioni su McAfee vengono fornite informazioni legali riguardanti McAfee Corporation.

Glossario

8

802.11

Insieme di standard IEEE per la tecnologia LAN senza fili. 802.11 specifica un'interfaccia over-the-air tra un client senza fili e una stazione di base o tra due client senza fili. Diverse specifiche di 802.11 includono 802.11a, uno standard per connessioni di rete fino a 54 Mbps nella banda dei 5 Ghz, 802.11b, uno standard per connessioni di rete fino a 11 Mbps nella banda dei 2,4 Ghz, 802.11g, uno standard per connessioni di rete fino a 54 Mbps nella banda dei 2,4 Ghz e 802.11i, una suite di standard di protezione per tutte le reti Ethernet senza fili.

802.11a

Estensione di 802.11 che si applica alle LAN senza fili e consente la trasmissione di dati fino a 54 Mbps nella banda dei 5 GHz. Nonostante la velocità di trasmissione sia superiore rispetto a 802.11b, la distanza coperta è di gran lunga inferiore.

802.11b

Estensione di 802.11 che si applica alle LAN senza fili e fornisce una velocità di trasmissione di 11 Mbps nella banda dei 2,4 GHz. 802.11b è attualmente considerato lo standard senza fili.

802.11g

Estensione di 802.11 che si applica alle LAN senza fili e fornisce fino a 54 Mbps nella banda dei 2,4 GHz.

802.1x

Non supportato da Wireless Home Network Security. Si tratta di uno standard IEEE per l'autenticazione su reti cablate e senza fili, ma viene utilizzato soprattutto per le reti senza fili basate su 802.11. Questo standard consente l'autenticazione avanzata reciproca fra i client e un server di autenticazione. Inoltre, 802.1x può fornire chiavi WEP dinamiche per utente e per sessione, diminuendo il carico amministrativo e i rischi per la protezione legati alle chiavi WEP statiche.

A

account di posta elettronica standard

La maggior parte degli utenti privati dispone di questo tipo di account. Vedere anche account POP3.

account MAPI

Acronimo di Messaging Application Programming Interface. Specifica di interfaccia di Microsoft che consente a differenti applicazioni di workgroup e messaggistica (tra cui posta elettronica, casella vocale e fax) di collaborare attraverso un singolo client, ad esempio il client di Exchange. Per questo motivo, il sistema MAPI è spesso utilizzato in ambienti aziendali in cui su utilizza Microsoft® Exchange Server. Molti utenti utilizzano tuttavia Microsoft Outlook per la posta elettronica Internet personale.

account MSN

Acronimo di Microsoft Network. Servizio online e portale Internet. Si tratta di un account basato sul Web.

account POP3

Acronimo di Post Office Protocol 3. La maggior parte degli utenti privati utilizza questo tipo di account. Si tratta della versione corrente dello standard Post Office Protocol utilizzato comunemente sulle reti TCP/IP. Anche noto come account di posta elettronica standard.

analisi immagini

Blocco della visualizzazione di immagini potenzialmente inappropriate. Le immagini sono bloccate per tutti gli utenti, ad eccezione dei membri appartenenti al gruppo di età dei maggiori di 18 anni.

archiviazione

Creazione di una copia dei file monitorati a livello locale su CD, DVD, unità USB, disco rigido esterno o unità di rete.

archiviazione

Creazione di una copia dei file monitorati a livello locale su CD, DVD, unità USB, disco rigido esterno o unità di rete.

archiviazione completa

Archiviazione completa di un set di dati in base ai tipi di file e ai percorsi monitorati impostati.

archiviazione rapida

Archiviazione solo dei file monitorati che sono cambiati dopo l'ultima archiviazione completa o rapida.

archivio del backup in linea

Percorso del server online dove sono memorizzati i file monitorati dopo che ne è stato eseguito il backup.

Archivio protetto password

Area di memorizzazione protetta per le password personali. che consente di memorizzare le password in modo tale che nessun altro utente, compreso un amministratore di McAfee o un amministratore di sistema, possa accedervi.

attacco brute force

Noto anche come brute force cracking. Si tratta di un metodo basato su tentativi ed errori utilizzato da applicazioni per decodificare dati crittografati come le password, applicando un grande dispendio di energie (mediante la forza bruta) anziché impiegare strategie mirate. Proprio come un criminale potrebbe forzare una cassaforte tentando tutte le combinazioni possibili, un'applicazione che utilizza la forza bruta procede attraverso la sequenza di tutte le possibili combinazioni di caratteri consentiti. L'uso della forza bruta è considerato un approccio infallibile anche se richiede tempi piuttosto lunghi.

attacco di tipo dictionary

Tipo di attacco in cui si tenta di individuare una password utilizzando una grande quantità di parole contenute in un elenco. I tentativi non vengono effettuati manualmente, ma mediante strumenti che tentano automaticamente di identificare la password.

attacco di tipo man-in-the-middle

L'autore dell'attacco intercetta i messaggi in uno scambio di chiavi pubbliche e li ritrasmette sostituendo la propria chiave pubblica a quella richiesta, in modo che le due parti originarie risultino ancora in comunicazione diretta tra loro. L'autore dell'attacco utilizza un programma che al client sembra il server e al server sembra il client. L'attacco può essere utilizzato semplicemente per ottenere accesso ai messaggi o per consentirne la modifica prima che siano ritrasmessi. Il termine deriva da un gioco in cui i partecipanti tentano di lanciarsi una palla mentre un altro giocatore nel mezzo tenta di afferrarla.

autenticazione

Processo di identificazione di un individuo, di solito basato su un nome utente e una password. L'autenticazione consente di verificare la veridicità dell'identità dichiarata dall'utente, ma non fornisce informazioni sui suoi diritti di accesso.

B

backup

Creazione di una copia dei file monitorati su un server online protetto.

browser

Programma client che utilizza il protocollo HTTP (Hypertext Transfer Protocol) per inviare richieste a server Web attraverso Internet. Un browser Web consente di rappresentare graficamente i contenuti.

chiave

Serie di lettere e/o numeri utilizzata da due dispositivi per autenticarne la comunicazione. Entrambi i dispositivi devono disporre della chiave. Vedere anche WEP, WPA, WPA2, WPA-PSK e WPA2- PSK.

client

Applicazione eseguita su PC o workstation che richiede un un server per l'esecuzione di alcune operazioni. Ad esempio, un client di posta elettronica è un'applicazione che consente l'invio e la ricezione di messaggi di posta elettronica.

client di posta elettronica

Account di posta elettronica. Ad esempio, Microsoft Outlook o Eudora.

compressione

Processo mediante il quale i dati (file) vengono compressi in un formato tale da ridurre al minimo lo spazio richiesto per memorizzarli o trasmetterli.

condivisione

Operazione che consente ai destinatari del messaggio di posta elettronica di accedere ai file di backup selezionati per un periodo limitato di tempo. Quando si condivide un file, la copia di backup del file viene inviata ai destinatari del messaggio di posta elettronica specificati. I destinatari ricevono un messaggio di posta elettronica da Data Backup in cui viene segnalato che i file sono stati condivisi. Nel messaggio di posta elettronica è riportato anche un collegamento ai file condivisi.

Controllo genitori

Impostazioni che permettono di configurare classificazioni dei contenuti, che limitano i siti Web e i contenuti visualizzabili da determinati utenti, e di impostare limiti temporali per l'accesso a Internet, che consentono di determinare i periodi in cui Internet sarà accessibile e la durata consentita della navigazione. Il controllo genitori consente inoltre di limitare l'accesso a siti Web specifici da parte di tutti gli utenti e di consentire o bloccare l'accesso in base a gruppi di età e a parole chiave ad essi associate.

cookie

Sul World Wide Web, un blocco di dati memorizzato su un client da un server Web. Quando l'utente visita nuovamente lo stesso sito Web, il browser invia una copia del cookie al server. I cookie vengono utilizzati per identificare gli utenti, richiedere al server l'invio di versioni personalizzate di determinate pagine Web, inviare informazioni sull'account dell'utente e per altri scopi di natura amministrativa.

I cookie consentono ai siti Web di memorizzare dati relativi agli utenti e di tenere traccia del numero di visite ricevute, dell'orario in cui le visite si sono verificate e delle pagine visualizzate. I cookie consentono inoltre agli utenti di personalizzare i siti Web. Molti siti Web richiedono un nome utente e una password per consentire l'accesso a determinate pagine e inviano un cookie al computer in modo che l'utente non debba effettuare l'accesso ogni volta. Tuttavia, i cookie possono essere utilizzati per attività dannose. Le società pubblicitarie online utilizzano spesso i cookie per determinare quali sono i siti più visitati da determinati utenti in modo da visualizzare informazioni pubblicitarie sui loro siti Web preferiti. Prima di consentire l'invio di cookie da parte di un sito, è consigliabile assicurarsi della sua affidabilità.

Benché siano una fonte di informazioni legittima, i cookie possono anche essere una fonte di informazioni per gli hacker. Molti siti Web per gli acquisti online memorizzano i dati relativi a carte di credito e altri dati personali nei cookie, in modo da facilitare le operazioni di acquisto dei clienti. Purtroppo possono verificarsi vulnerabilità della protezione che consentono agli hacker di accedere ai dati presenti nei cookie memorizzati nei computer dei clienti.

crittografia

Processo mediante il quale i dati vengono trasformati da testo in codice, oscurando le informazioni per renderle illeggibili agli utenti che non sanno come decifrarle.

D

Denial of Service (Negazione del servizio)

Su Internet, un attacco DoS (Denial of Service, Negazione del servizio) è un incidente durante il quale un utente o un'organizzazione vengono privati dei servizi di una risorsa solitamente disponibile. Di solito, la negazione di un servizio è costituita dalla mancata disponibilità di un particolare servizio di rete, ad esempio la posta elettronica, oppure dalla perdita temporanea di tutti i servizi e della connettività di rete. Nei casi peggiori, ad esempio, un sito Web a cui accedono milioni di persone può essere occasionalmente forzato a interrompere temporaneamente il funzionamento. Un attacco DoS può anche provocare la distruzione di programmi e di file in un sistema informatico. Per quanto di solito siano intenzionali e pericolosi, gli attacchi DoS possono talvolta verificarsi accidentalmente. Un attacco DoS è un tipo di violazione della protezione di un sistema informatico che di solito non comporta il furto di informazioni o altre perdite di protezione. Tuttavia, questi attacchi possono costare alla persona o all'azienda che li riceve una gran quantità di tempo e denaro.

disco rigido esterno

Disco rigido collegato all'esterno del computer .

DNS

Acronimo di Domain Name System. Sistema gerarchico che consente agli host presenti su Internet di disporre sia di indirizzi del nome di dominio (ad esempio bluestem.prairienet.org) che di indirizzi IP (ad esempio 192.17.3.4). L'utente utilizza l'indirizzo del nome del dominio, il quale viene tradotto automaticamente nell'indirizzo IP numerico, il quale viene a sua volta utilizzato dal software di instradamento dei pacchetti. I nomi DNS sono costituiti da un dominio di primo livello (ad esempio .com, .org e .net), un dominio di livello secondario (il nome del sito di un'azienda, di un'organizzazione o di un privato) ed eventualmente da uno o più sottodomini (server all'interno di un dominio di secondo livello). Vedere anche server DNS e indirizzo IP.

dominio

Indirizzo di una connessione di rete che consente l'identificazione del titolare dell'indirizzo in un formato gerarchico: server.organizzazione.tipo. Ad esempio, www.whitehouse.gov identifica il server Web della Casa bianca (White House), che fa parte del governo degli Stati Uniti.

E

elenco indirizzi autorizzati

Elenco di siti Web a cui è consentito l'accesso perché non considerati dannosi.

elenco indirizzi bloccati

Elenco di siti Web considerati dannosi. Un sito Web può essere inserito in un elenco di indirizzi bloccati perché su di esso vengono eseguite operazioni fraudolente o perché sfrutta vulnerabilità del browser per inviare all'utente programmi potenzialmente indesiderati.

ESS (Extended Service Set)

Insieme di una o più reti che formano un'unica sottorete.

evento

Eventi provenienti da 0.0.0.0

Due sono le cause più probabili per il rilevamento di eventi provenienti dall'indirizzo IP 0.0.0.0. La prima causa, quella più comune, è che per qualche motivo il computer ha ricevuto un pacchetto non valido. Internet non è sempre affidabile al 100% ed è quindi possibile che vengano inoltrati pacchetti non validi. Poiché i pacchetti vengono esaminati da Firewall prima della convalida da parte di TCP/IP, è possibile che questi pacchetti vengano segnalati come evento.

In altri casi è possibile che sia stato effettuato lo spoofing dell'indirizzo IP di origine, ossia che quest'ultimo sia stato contraffatto. I pacchetti contraffatti potrebbero indicare che è in corso una scansione per la ricerca di Trojan e che è stato effettuato un tentativo sul computer in uso. È importante ricordare che Firewall blocca tali tentativi.

Eventi provenienti da 127.0.0.1

Alcuni eventi vengono generati dall'indirizzo IP 127.0.0.1. Si tratta di un indirizzo IP speciale, noto come indirizzo di loopback.

Indipendentemente dal computer in uso, 127.0.0.1 si riferisce sempre al computer locale. È anche possibile fare riferimento a tale indirizzo come localhost, poiché il nome di computer localhost viene sempre risolto nell'indirizzo IP 127.0.0.1. È comunque poco probabile che il computer stia tentando di attaccare se stesso oppure sia controllato da un Trojan o da spyware. Molti programmi legittimi utilizzano infatti l'indirizzo di loopback per la comunicazione fra i componenti. Ad esempio, molti server di posta o server Web personali possono essere configurati utilizzando un'interfaccia Web in genere accessibile mediante l'indirizzo http://localhost/.

Il traffico proveniente da tali programmi viene tuttavia autorizzato da Firewall. Quindi, se si rilevano eventi provenienti dall'indirizzo 127.0.0.1, è probabile che sia stato effettuato lo spoofing dell'indirizzo IP di origine, ossia che questo sia stato contraffatto. I pacchetti contraffatti indicano che è in corso una scansione per la ricerca di Trojan. È importante ricordare che Firewall blocca tali tentativi. È evidente che la segnalazione di eventi provenienti da 127.0.0.1 non è di alcuna utilità e, pertanto, non viene eseguita.

Esistono tuttavia programmi, come Netscape 6.2 e versioni successive, che richiedono l'aggiunta di 127.0.0.1 all'elenco degli **indirizzi IP affidabili**. La modalità di comunicazione tra i componenti di tali programmi non consente a Firewall di determinare se si tratti di traffico locale.

Nel caso di Netscape 6.2, se non si imposta 127.0.0.1 come affidabile, non sarà possibile utilizzare l'elenco degli amici. Se si rileva quindi traffico proveniente da 127.0.0.1 e tutti i programmi del computer funzionano normalmente, è possibile bloccare tale traffico senza che si verifichino problemi. Se, tuttavia, in un programma, ad esempio Netscape, si verificano problemi, aggiungere 127.0.0.1 all'elenco degli **indirizzi IP affidabili** di Firewall, quindi verificare se i problemi sono stati risolti.

Se l'inserimento di 127.0.0.1 nell'elenco degli **indirizzi IP affidabili** consente di risolvere il problema, è necessario valutare le opzioni disponibili: se si imposta 127.0.0.1 come affidabile, il programma funzionerà correttamente, ma il sistema sarà più vulnerabile ad attacchi di spoofing. Se non si imposta l'indirizzo come affidabile, il programma non funzionerà correttamente, ma si sarà protetti dal traffico dannoso.

Eventi proveninenti dai computer della LAN

Per la maggior parte delle impostazioni LAN in uso nelle aziende, è possibile considerare come affidabili tutti i computer presenti sulla LAN.

Eventi provenienti da indirizzi IP privati

Gli indirizzi IP con formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 sono detti non instradabili o privati. Tali indirizzi IP non dovrebbero mai lasciare la rete e possono essere considerati quasi sempre affidabili.

Il blocco 192.168 viene utilizzato con Condivisione connessione Internet di Microsoft. Se si utilizza Condivisione connessione Internet e si rilevano eventi provenienti da tale blocco di indirizzi IP, è possibile aggiungere l'indirizzo IP 192.168.255.255 all'elenco degli **indirizzi IP affidabili**. In tal modo verrà impostato come affidabile l'intero blocco 192.168.xxx.xxx.

Se non si è connessi a una rete privata e si rilevano eventi provenienti da questi intervalli di indirizzi IP, è possibile che gli indirizzi IP di origine siano stati sottoposti a spoofing, ovvero che siano stati contraffatti. I pacchetti contraffatti indicano solitamente che è in corso una scansione per la ricerca di Trojan. È importante ricordare che Firewall blocca tali tentativi.

Poiché gli indirizzi IP privati sono separati dagli indirizzi IP in Internet, la segnalazione di tali eventi risulta inutile, quindi non viene effettuata.

firewall

Sistema progettato per impedire l'accesso non autorizzato a o da una rete privata. I firewall possono essere implementati sia nell'hardware che nel software o con una combinazione di entrambi. I firewall vengono utilizzati di frequente per impedire a utenti di Internet non autorizzati di accedere a reti private connesse a Internet, specialmente a una rete Intranet. Tutti i messaggi in ingresso o in uscita da una rete Intranet passano attraverso il firewall. Il firewall esamina tutti i messaggi e blocca quelli non conformi ai criteri di protezione specificati. Un firewall è considerato la prima linea di difesa nella protezione delle informazioni private. Per una maggiore protezione, è possibile crittografare i dati.

gateway integrato

Dispositivo che combina le funzioni di punto di accesso, router e firewall. Alcuni dispositivi possono persino includere funzionalità avanzate di protezione e bridging.

gruppi di classificazione del contenuto

Gruppi di età a cui appartiene un utente. Il contenuto viene classificato (ossia, reso disponibile o bloccato) in base al gruppo di classificazione del contenuto al quale appartiene l'utente. I gruppi di classificazione del contenuto comprendono: minori di 6 anni, 6 - 9 anni, 10 - 13 anni, 14 - 18 anni, maggiori di 18 anni.

hotspot

Specifico luogo geografico in cui un punto di accesso fornisce a visitatori che dispongono di dispositivi portatili servizi pubblici di rete a banda larga attraverso una rete senza fili. Gli hotspot si trovano spesso in luoghi particolarmente affollati come gli aeroporti, le stazioni ferroviarie, le biblioteche, i porti marittimi, i centri congressuali e gli alberghi. Di solito la loro portata di accesso è limitata.

Indirizzo IP

L'indirizzo del protocollo Internet, o indirizzo IP, è un numero univoco costituito da quattro parti separate da punti, ad esempio 63.227.89.66. In Internet, a ogni computer, dal server più grande a un portatile che comunica attraverso un telefono cellulare, è assegnato un indirizzo IP univoco. Non tutti i computer dispongono di un nome di dominio, ma tutti dispongono di un indirizzo IP.

Di seguito sono elencati alcuni tipi di indirizzi IP speciali:

- Indirizzi IP non instradabili. Tali indirizzi sono noti anche come spazi IP privati e non possono essere utilizzati su Internet. I blocchi privati sono 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.
- Indirizzi IP di loopback**:** gli indirizzi di loopback vengono utilizzati a scopo di test. Il traffico inviato a questo blocco di indirizzi IP torna subito al dispositivo che genera il pacchetto, non lascia mai il dispositivo e viene utilizzato principalmente per test di hardware e software. Il blocco degli indirizzi IP di loopback è 127.x.x.x.

Indirizzo IP nullo: si tratta di un indirizzo non valido. Se risulta visibile, ciò indica che l'indirizzo IP da cui proveniva o a cui era destinato il traffico era vuoto. Ovviamente, tale situazione non è normale e indica spesso che l'origine del traffico viene deliberatamente nascosta dal mittente. Il mittente non sarà in grado di ricevere risposte, a meno che il pacchetto non venga ricevuto da un'applicazione in grado di comprenderne i contenuti, in cui devono essere incluse istruzioni specifiche per tale applicazione. Qualsiasi indirizzo che inizi per 0 (0.x.x.x) è un indirizzo nullo. Ad esempio, 0.0.0.0 è un indirizzo IP nullo.

Indirizzo MAC (Media Access Control Address)

Indirizzo di basso livello assegnato al dispositivo fisico che accede alla rete.

Internet

Internet è un sistema costituito da un numero elevatissimo di reti interconnesse che utilizzano i protocolli TCP/IP per individuare e trasferire dati. Internet è l'evoluzione di una rete di computer di università e college creata tra la fine degli anni '60 e l'inizio degli annu '70 dal Dipartimento della difesa degli Stati Uniti e denominata ARPANET. Internet è oggi una rete globale costituita da circa 100.000 reti indipendenti.

intestazione

Informazioni aggiunte a una porzione di un messaggio nel corso del ciclo di vita del messaggio stesso. L'intestazione contiene indicazioni relative alla modalità di consegna del messaggio da parte del software Internet, all'indirizzo cui inviare la risposta, un identificatore univoco per il messaggio di posta elettronica e altre informazioni amministrative. Esempi dei campi dell'intestazione sono: To, From, Cc, Date, Subject, Message-ID e Received.

intranet

Rete privata, situata in genere all'interno di un'organizzazione, il cui funzionamento è molto simile a quello di Internet. È divenuto abituale consentire l'accesso alle reti Intranet da computer autonomi utilizzati da studenti o dipendenti dall'esterno dell'università o del luogo di lavoro. Firewall, procedure di accesso e password hanno lo scopo di garantirne la protezione.

LAN (Local Area Network)

Rete di computer che si estende in un'area relativamente ridotta. Molte LAN sono ristrette a un solo edificio o gruppo di edifici. Tuttavia, una LAN può essere connessa ad altre LAN a qualunque distanza tramite telefono e onde radio. Un sistema di LAN connesse in questo modo è detto WAN (Wide-Area Network). Nella maggior parte delle LAN, workstation e PC sono connessi fra di loro, di solito mediante semplici hub o switch. Ciascun nodo (singolo computer) in una LAN dispone della propria CPU che utilizza per l'esecuzione di programmi, ma è anche in grado di accedere a dati e a dispositivi (ad esempio le stampanti) presenti in qualsiasi punto della LAN. In tal modo, molti utenti possono condividere dispositivi costosi, come le stampanti laser, nonché i dati. Gli utenti, inoltre, possono utilizzare la LAN per comunicare tra di loro, ad esempio inviando messaggi di posta elettronica o avviando sessioni di chat.

larghezza di banda

Quantità di dati trasmettibili in un determinato lasso di tempo. Per i dispositivi digitali, la larghezza di banda di solito viene espressa in bit per secondo (bps) o byte per secondo. Per i dispositivi analogici, la larghezza di banda viene espressa in cicli per secondo o Hertz (Hz).

libreria

Area di memorizzazione online per i file pubblicati dagli utenti di Data Backup. La libreria è un sito Web su Internet, accessibile a chiunque disponga di un accesso a Internet.

MAC (Media Access Control o Message Authenticator Code)

Per il primo significato, vedere Indirizzo MAC. Il secondo è un codice utilizzato per identificare un determinato messaggio (ad esempio, un messaggio RADIUS). Il codice generalmente è un hash dei contenuti del messaggio ottenuto mediante crittografia avanzata, che include un valore univoco per garantire una protezione contro la riproduzione.

mappa di rete

In Network Manager, rappresentazione grafica dei computer e dei componenti che costituiscono la rete domestica.

NIC (Network Interface Card)

Scheda che si inserisce in un laptop o in altro dispositivo e consente la connessione del dispositivo alla LAN.

nodo

Singolo computer connesso a una rete.

parola chiave

Parola che è possibile assegnare a un file di backup per stabilire un rapporto o una connessione con altri file a cui è stata assegnata la stessa parola chiave. L'assegnazione di parole chiave ai file agevola la ricerca dei file che sono stati pubblicati su Internet.

password

Codice, in genere alfanumerico, utilizzato per ottenere l'accesso a un computer, a un determinato programma o a un sito Web.

percorsi monitorati

Cartelle sul computer monitorate da Data Backup.

percorso di monitoraggio approfondito

Una cartella sul computer sottoposta, insieme a tutte le sue sottocartelle, al monitoraggio delle modifiche da parte di Data Backup. Se si imposta un percorso di monitoraggio approfondito, Data Backup esegue il backup dei tipi di file monitorati in tale cartella e nelle relative sottocartelle.

percorso di monitoraggio rapido

Cartella sul computer sottoposta al monitoraggio delle modifiche da parte di Data Backup. Se si imposta un percorso di monitoraggio rapido, Data Backup esegue il backup dei tipi di file monitorati all'interno della cartella, ignorando il contenuto delle sottocartelle.

phishing

Il termine, che si pronuncia "fishing", si riferisce a sistemi ingannevoli utilizzati per il furto di dati riservati quali il numero della carta di credito e del codice fiscale, l'ID utente e le password. Le potenziali vittime ricevono un messaggio di posta elettronica che ha l'aspetto di un messaggio inviato dal loro provider di servizi Internet, dalla loro banca o da un loro rivenditore di fiducia. I messaggi di posta elettronica possono essere inviati a utenti selezionati da un elenco o scelti in maniera casuale, nel tentativo di individuare una percentuale di essi che disponga effettivamente di un account presso l'organizzazione legittima.

popup

Piccole finestre che vengono visualizzate davanti ad altre finestre sullo schermo del computer. Le finestre popup sono spesso utilizzate nei browser Web per visualizzare annunci pubblicitari. McAfee blocca le finestre popup caricate automaticamente sul browser insieme a una pagina Web, ma non blocca le finestre popup che vengono caricate quando si seleziona un collegamento.

porta

Punto in cui i dati entrano e/o escono dal computer. Ad esempio, il tradizionale modem analogico viene connesso alla porta seriale. Nelle comunicazioni TCP/IP i numeri di porta sono valori virtuali utilizzati per suddividere il traffico in flussi associati ad applicazioni specifiche. Le porte sono assegnate a protocolli standard, quali SMTP o HTTP, in modo che ai programmi sia nota la porta sulla quale tentare di stabilire una connessione. La porta di destinazione per i pacchetti TCP indica l'applicazione o il server desiderato.

posta elettronica

Posta elettronica, messaggi inviati tramite Internet o all'interno della rete LAN o WAN di un'azienda. Gli allegati di posta elettronica sotto forma di file EXE (eseguibili) o file VBS (script di Visual Basic) sono diventati un mezzo sempre più diffuso per la trasmissione di virus e Trojan.

PPPoE

Point-to-Point Protocol Over Ethernet (Protocollo punto a punto su Ethernet). Utilizzato da molti provider DSL, PPPoE supporta i livelli di protocollo e l'autenticazione ampiamente utilizzati in PPP e consente di stabilire connessioni punto-punto nell'architettura Ethernet, solitamente multipunto.

programma potenzialmente indesiderato

I programmi potenzialmente indesiderati comprendono spyware, adware e altri programmi che raccolgono e trasmettono dati personali senza autorizzazione.

protocollo

Formato concordato per la trasmissione di dati tra due dispositivi. Dal punto di vista di un utente, l'unico aspetto rilevante dei protocolli è che il computer o il dispositivo deve supportare quelli appropriati, se desidera comunicare con altri computer. Il protocollo può essere implementato nell'hardware o nel software.

proxy

Computer o software che separa una rete da Internet, presentando un solo indirizzo di rete ai siti esterni. Agendo come intermediario per tutti i computer interni, il proxy protegge le identità di rete pur continuando a fornire l'accesso a Internet. Vedere anche Server proxy.

pubblicazione

Operazione il cui scopo è rendere un file di backup disponibile a tutti su Internet.

Punto di accesso (AP, Access Point)

Dispositivo di rete che consente ai client 802.11 di connettersi a una rete locale (LAN). I punti di accesso estendono la gamma fisica di servizi per gli utenti di dispositivi senza fili. Talvolta sono denominati router senza fili.

Punto di accesso pericoloso

Punto di accesso di cui un'azienda non autorizza il funzionamento. Questo tipo di punto di accesso spesso non è conforme ai criteri di protezione della LAN senza fili (WLAN). Un punto di accesso pericoloso attiva un'interfaccia alla rete aziendale non protetta e aperta accessibile dall'esterno della struttura fisicamente controllata.

All'interno di una WLAN correttamente protetta, i punti di accesso pericolosi sono più dannosi degli utenti non autorizzati. Se sono attivi dei meccanismi di autenticazione efficaci, è improbabile che utenti non autorizzati che tentano l'accesso a una WLAN riescano a raggiungere importanti risorse aziendali. Maggiori problemi sorgono, tuttavia, quando un dipendente o un hacker si collegano utilizzando un punto di accesso pericoloso. Questo, infatti, consente l'accesso alla rete aziendale a chiunque disponga di un dispositivo dotato di 802.11, consentendogli di avvicinarsi a risorse critiche.

quarantena

Se vengono rilevati file sospetti, essi vengono messi in quarantena. È quindi possibile intraprendere le opportune azioni in un secondo momento.

RADIUS (Remote Access Dial-In User Service)

Protocollo che fornisce l'autenticazione degli utenti, di solito in un contesto di accesso remoto. Inizialmente definito per l'uso con i server di accesso remoto dial-in, il protocollo viene ora utilizzato in un'ampia gamma di ambienti di autenticazione, inclusa l'autenticazione 802.1x del segreto condiviso di un utente di una WLAN.

rete

Quando si connettono due o più computer, si crea una rete.

rete gestita

Rete domestica con due tipi di membri: membri gestiti e membri non gestiti. I membri gestiti, diversamente da quelli non gestiti, consentono agli altri computer in rete di monitorare lo stato delle protezione McAfee.

ripristino

Recupero di una copia di un file dall'archivio del backup in linea o da un archivio.

roaming

Capacità di spostarsi da un'area coperta da un punto di accesso a un'altra senza interruzione di servizio o perdita di connettività.

router

Dispositivo di rete che inoltra pacchetti da una rete all'altra. Sulla base di tabelle di instradamento interne, i router leggono ogni pacchetto in ingresso e decidono come inoltrarlo. L'interfaccia del router alla quale i pacchetti in uscita vengono inviati può essere determinata dalla combinazione dell'indirizzo di origine e di destinazione, nonché dalle attuali condizioni di traffico, qiali il carico, i costi della linea e il cattivo stato della linea. Talvolta sono denominati punti di accesso.

scansione in tempo reale

Scansione dei file alla ricerca di virus o altre attività quando vengono aperti dall'utente o dal computer.

scheda di rete senza fili

Contiene i circuiti che consentono a un computer o altri dispositivi di comunicare con un router senza fili (collegamento a una rete senza fili). Le schede di rete senza fili possono essere incorporate nei circuiti principali di un dispositivo hardware oppure essere costituite da un componente aggiuntivo a parte da inserire nel dispositivo mediante un'apposita porta.

schede senza fili PCI

Consentono di connettere un computer desktop a una rete. La scheda si inserisce in uno slot di espansione PCI all'interno del computer.

schede senza fili USB

Forniscono un'interfaccia seriale Plug and Play espandibile. Questa interfaccia fornisce una connessione senza fili standard e a basso costo per periferiche come tastiere, mouse, joystick, stampanti, scanner, dispositivi di archiviazione e videocamere per conferenze.

script

Gli script possono creare, copiare o eliminare file. Sono anche i grado di aprire il registro di sistema di Windows.

segreto condiviso

Vedere anche RADIUS. Protegge parti riservate dei messaggi RADIUS. Il segreto condiviso è una password che può essere condivisa dall'autenticatore e dal server di autenticazione in maniera protetta.

server

Computer o software che fornisce servizi specifici al software in esecuzione su altri computer. Il "server di posta" presso il provider di servizi Internet è il software che gestisce tutta la posta in arrivo e in uscita per tutti gli utenti del provider. Un server in una LAN è l'hardware che costituisce il nodo primario della rete. Può anche disporre di software che fornisce servizi specifici, dati o altre funzionalità a tutti i computer client collegati.

server DNS

Abbreviazione per server Domain Name System. Computer in grado di rispondere a query DNS (Domain Name System). Sul server DNS è presente un database in cui sono memorizzati i computer host e i corrispondenti indirizzi IP. Se, ad esempio, al server DNS viene inviato il nome apex.com, esso restituirà l'indirizzo IP della società ipotetica Apex. Chiamato anche: server dei nomi. Vedere anche DNS e indirizzo IP.

server proxy

Componente del firewall che gestisce il traffico Internet da e verso una LAN (Local Area Network). Un server proxy consente di migliorare le prestazioni fornendo i dati richiesti frequentemente, ad esempio una pagina Web, e di filtrare ed eliminare le richieste non considerate appropriate, quali le richieste di accesso non autorizzato ai file proprietari.

server SMTP

Acronimo di Simple Mail Transfer Protocol. Protocollo TCP/IP per l'invio di messaggi da un computer a un altro su una rete. Questo protocollo è utilizzato su Internet per instradare i messaggi di posta elettronica.

sincronizzazione

Risoluzione di eventuali incoerenze tra i file di backup e quelli memorizzati sul computer locale. La sincronizzazione è necessaria quando la versione di un file presente nell'archivio del backup in linea è più recente rispetto a quella del file memorizzato negli altri computer. Mediante la sincronizzazione, la copia del file memorizzata sui computer viene aggiornata con la versione del file presente nell'archivio del backup in linea.

sovraccarico del buffer

I sovraccarichi del buffer si verificano quando programmi o processi sospetti tentano di memorizzare in un buffer (area di memorizzazione temporanea dei dati) del computer una quantità di dati superiore al limite consentito, causando il danneggiamento o la sovrascrittura di dati validi presenti nei buffer adiacenti.

spoofing degli indirizzi IP

Contraffazione di indirizzi IP in un pacchetto IP. Viene utilizzato in molti tipi di attacchi, inclusa la presa di controllo della sessione. Viene inoltre impiegato per contraffare le intestazioni dei messaggi di posta indesiderati in modo da impedire la corretta individuazione dei mittenti.

SSID (Service Set Identifier)

Nome di rete per i dispositivi in un sottosistema LAN senza fili. Si tratta di una stringa di testo non crittografata, contenente 32 caratteri, aggiunta all'inizio di ogni pacchetto WLAN. L'SSID differenzia una WLAN dall'altra, per cui tutti gli utenti di una rete devono fornire lo stesso SSID per accedere a un determinato punto di accesso. L'SSID impedisce l'accesso a qualsiasi dispositivo client che non disponga di dello stesso SSID. Tuttavia, per impostazione predefinita un punto di accesso trasmette il proprio SSID nel proprio beacon. Anche se la trasmissione dell'SSID è disattivata, un hacker può rilevare l'SSID attraverso lo sniffing.

SSL (Secure Sockets Layer)

Protocollo sviluppato da Netscape per la trasmissione di documenti privati tramite Internet. L'SSL funziona utilizzando una chiave pubblica per crittografare i dati trasferiti sulla connessione SSL. Sia Netscape Navigator che Internet Explorer utilizzano e supportano SSL e molti siti Web utilizzano il protocollo per ottenere informazioni riservate dagli utenti, come i numeri di carta di credito. Per convenzione, gli URL che richiedono una connessione SSL iniziano con https: invece di http:.

SystemGuard

I moduli SystemGuard rilevano le modifiche non autorizzate subite dal computer e visualizzano un messaggio quando tali modifiche vengono apportate.

testo crittografato

Dati crittografati. Il testo crittografato è illeggibile finché non viene convertito in testo normale (decrittografato) mediante una chiave.

testo normale

Qualsiasi messaggio non crittografato.

tipi di file monitorati

Tipi di file, ad esempio DOC, XLS e così via, di cui Data Backup esegue il backup o memorizza negli archivi all'interno dei percorsi monitorati.

TKIP (Temporal Key Integrity Protocol)

Metodo di correzione rapida per superare la debolezza inerente alla protezione WEP, in particolare il riutilizzo delle chiavi crittografiche. TKIP modifica le chiavi temporali ogni 10.000 pacchetti, fornendo un metodo di distribuzione dinamica che migliora notevolmente la protezione della rete. Il processo (di protezione) TKIP inizia con una chiave temporale da 128 bit condivisa tra client e punti di accesso. TKIP combina la chiave temporale con l'indirizzo MAC (del computer client) e aggiunge un vettore di inizializzazione da 16 ottetti, relativamente grande, per produrre la chiave utilizzata per la crittografia dei dati. Questa procedura assicura che ogni stazione utilizzi flussi di chiavi differenti per crittografare i dati. TKIP utilizza RC4 per eseguire la crittografia. Anche WEP utilizza RC4.

Trojan horse

I Trojan horse sono programmi che si presentano sotto forma di applicazioni innocue. I Trojan horse non sono virus in quanto non duplicano se stessi, ma possono essere altrettanto distruttivi.

unità di rete

Unità disco o nastro collegata a un server su una rete e condivisa da più utenti. Le unità di rete sono spesso chiamate unità remote.

URL

Uniform Resource Locator. Formato standard degli indirizzi Internet.

VPN (Virtual Private Network)

Rete costruita utilizzando cavi pubblici per l'unione di nodi. Ad esempio, esistono molti sistemi che consentono di creare reti utilizzando Internet come mezzo di trasmissione dei dati. Tali sistemi utilizzano la crittografia e altri meccanismi di protezione per garantire che solo gli utenti autorizzati possano accedere alla rete e che i dati non possano essere intercettati.

wardriver

Intrusi armati di laptop, software speciale e hardware di fortuna che girano per città, sobborghi e zone industriali per intercettare il traffico di LAN senza fili.

Web bug

Piccoli file grafici che si incorporano autonomamente nelle pagine HTML e consentono a un'origine non autorizzata di impostare cookie sul computer dell'utente. I cookie possono quindi trasmettere dati all'origine non autorizzata. I Web bug sono anche chiamati Web beacon, pixel tag, GIF trasparenti o GIF invisibili.

WEP (Wired Equivalent Privacy)

Protocollo di crittografia e autenticazione definito come parte dello standard 802.11. Le versioni iniziali sono basate su crittografia RC4 e sono caratterizzate da una notevole vulnerabilità. WEP tenta di fornire la protezione crittografando i dati su onde radio, in modo che siano protetti durante la trasmissione fra due punti. Tuttavia, si è scoperto che WEP non è tanto sicuro come si credeva.

Wi-Fi (Wireless Fidelity)

Utilizzato genericamente quando ci si riferisce a qualunque tipo di rete 802.11, che sia 802.11b, 802.11a, dual-band, ecc. Il termine è utilizzato da Wi-Fi Alliance.

Wi-Fi Alliance

Organizzazione costituita da fornitori leader di software e dispositivi senza fili con la missione di (1) certificare l'interoperabilità di tutti i prodotti basati su 802.11 e di (2) promuovere il termine Wi-Fi come nome di marchio globale in tutti i mercati per qualsiasi prodotto LAN senza fili basato su 802.11. L'organizzazione funge da consorzio, laboratorio di collaudo e centro di raccolta e smistamento per i fornitori che desiderano promuovere l'interoperabilità e lo sviluppo di questo settore.

Mentre tutti i prodotti 802.11a/b/g sono detti Wi-Fi, solo i prodotti che hanno superato la verifica Wi-Fi Alliance possono essere definiti Wi-Fi Certified (un marchio registrato). I prodotti che hanno superato la verifica sono contrassegnati da un sigillo di identificazione sulla confezione che segnala il prodotto come Wi-Fi Certified e che indica la banda di frequenza radio utilizzata. Questo gruppo prima era noto con il nome di Wireless Ethernet Compatibility Alliance (WECA), ma ha modificato il nome nell'ottobre 2002 per rispecchiare meglio il marchio Wi-Fi che desidera costruire.

Wi-Fi Certified

Tutti i prodotti collaudati e approvati come Wi-Fi Certified (un marchio registrato) da Wi-Fi Alliance sono reciprocamente iteroperativi, anche se realizzati da produttori diversi. Un utente che dispone di un prodotto Wi-Fi Certified può utilizzare un punto di accesso di qualunque marca con hardware client di qualsiasi altra marca, purché siano certificati. Tuttavia, in genere, tutti i prodotti Wi-Fi che utilizzano la stessa frequenza radio (ad esempio, 2,4 GHz per 802.11b o 11g, 5 GHz per 802.11a) di altri prodotti funzionano senza problemi, anche se non sono Wi-Fi Certified.

WLAN (Wireless Local Area Network)

Vedere anche LAN. Rete locale che utilizza supporto senza fili per le connessioni. In una WLAN, per la comunicazione tra nodi, vengono utilizzate onde radio ad alta frequenza anziché cavi.

worm

Un worm è un virus in grado di autoreplicarsi; esso risiede nella memoria attiva e può inviare copie di sé stesso attraverso la posta elettronica. I worm si replicano e utilizzano le risorse di sistema, rallentando o bloccando i programmi.

WPA (Wi-Fi Protected Access)

Standard di specifiche che aumenta notevolmente il livello di protezione dei dati e il controllo dell'accesso dei sistemi LAN senza fili, esistenti e futuri. Progettato per funzionare sull'hardware esistente come upgrade software, WPA è derivato dallo standard IEEE 802.11i ed è compatibile con esso. Se correttamente installato, garantisce agli utenti della LAN senza fili un elevato livello di protezione dei dati e che l'accesso alla rete venga effettuato solo da utenti autorizzati.

WPA-PSK

Una speciale modalità WPA progettata per gli utenti privati che non richiedono una protezione avanzata a livello enterprise e non hanno accesso a server di autenticazione. Utilizzando questa modalità, l'utente privato inserisce manualmente la password iniziale per attivare l'accesso protetto Wi-Fi in modalità PSK (Pre-Shared Key, Chiave già condivisa) e deve cambiare regolarmente la passphrase su ciascun punto di accesso e computer senza fili. Vedere anche WPA2-PSK e TKIP.

WPA2

Vedere anche WPA. WPA2 è un aggiornamento dello standard di protezione WPA e si basa sullo standard IEEE 802.11i.

WPA2-PSK

Vedere anche WPA-PSK e WPA2. WPA2-PSK è simile al WPA-PSK e si basa sullo standard WPA2. Una funzione comune di WPA2-PSK è che i dispositivi spesso supportano più modalità di crittografia (ad esempio AES, TKIP) contemporaneamente, mentre i dispositivi più obsoleti supportano generalmente solo una singola modalità di crittografia alla volta (ossia, tutti i client devono utilizzare la stessa modalità di crittografia).

Informazioni su McAfee

McAfee, Inc., con sede centrale a Santa Clara, California, e leader globale nella gestione dei rischi legati alla prevenzione delle intrusioni e alla protezione, offre soluzioni e servizi dinamici e affidabili che proteggono sistemi e reti di tutto il mondo. Grazie alla sua insuperata esperienza in materia di protezione e al suo impegno in termini di innovazione, McAfee offre agli utenti privati, alle aziende, al settore pubblico e ai provider di servizi la capacità di bloccare gli attacchi, di impedire le interruzioni e di controllare e migliorare continuamente la protezione dei loro computer.

Copyright

Indice

L

M

N

P

Q

R

S

T

U

V

W